Quantum algorithms for classical lattice models

G. De las Cuevas and W. Dür

Institut für Theoretische Physik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria
Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie der Wissenschaften, Innsbruck, Austria

M. Van den Nest

Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D-85748 Garching, Germany

M. A. Martin–Delgado

Departamento de Física Teórica I, Universidad Complutense, 28040 Madrid, Spain
(Dated: January 19, 2013)

We give efficient quantum algorithms to estimate the partition function of (i) the six vertex model on a two–dimensional (2D) square lattice, (ii) the Ising model with magnetic fields on a planar graph, (iii) the Potts model on a quasi 2D square lattice, and (iv) the $\mathbb{Z}_2$ lattice gauge theory on a three–dimensional square lattice. Moreover, we prove that these problems are BQP–complete, that is, that estimating these partition functions is as hard as simulating arbitrary quantum computation. The results are proven for a complex parameter regime of the models. The proofs are based on a mapping relating partition functions to quantum circuits introduced in [Van den Nest *et al.* Phys. Rev. A **80**, 052334 (2009)] and extended here.

I. INTRODUCTION

Ising models are paradigmatic in analytical and numerical studies of phase transitions [1, 2]. Their virtue is being simple enough to handle but nonetheless complex enough to capture the relevant physics. The same is true for other emblematic classical spin models, like the Potts model [3], or the six vertex model [4], which serve as toy models for certain physical systems. As a matter of fact, their applicability extends beyond physics, since spin models are used in the study of neural networks [5], biology [5] and, more generally, statistical mechanical tools are also applied in economics [6]. The reason lies in the fact that these models study classical degrees of freedom ("spins") which interact with each other (possibly in many–body interactions), and this general scheme can serve as an abstract model for a wide class of systems.

The central problem in the study of these models in equilibrium is the computation of their partition function $\mathcal{Z} := \sum_{\mathbf{s}} e^{-\beta H(\mathbf{s})}$, where $H(\mathbf{s})$ is the Hamiltonian (or: "energy function"), β is defined as $\beta := 1/(k_B T)$ where k_B is Boltzmann's constant and T is the temperature, and $\mathbf{s}$ is the spin configuration. As is well known in statistical mechanics, this function captures all relevant physical properties, since any thermodynamical quantity (such as the magnetization or the mean energy) can be derived as a function of $\mathcal{Z}$ [7]. In other words, knowledge of $\mathcal{Z}$ as a function of the parameters of the system amounts to complete knowledge of the thermal properties of the system. Thus, it is natural to investigate the computational complexity (colloquially speaking: the effort in terms of resources) required to compute or approximate $\mathcal{Z}$. The emblematic models mentioned above have received most of the attention in this direction. For

example, for the Ising model, Barahona [4] showed that computing its partition function in three dimensions (3D) is computationally very hard—to be precise, it is #P–complete, which is, colloquially speaking, the counting version of NP [8]. This was an important contribution that settled the issue for those trying to tackle the problem after Onsager's success in solving the Ising model in two dimensions (2D) [9].

Further, one can raise the question of how hard it is to compute the partition function of these models on a *quantum* computer. Quantum computers are known to offer a speedup over their classical counterparts in certain algorithms. Notably, the factoring problem is known to be feasible by a quantum computer [10], while it remains intractable in all known classical algorithms. Roughly speaking, 'feasible' means that the resources (in time and space) required to solve it scale polynomially with the size of the input of the problem, and intractable means that they may scale exponentially. The quantum computational complexity of classical spin models has been addressed, for example, in [11], where a quantum algorithm for the Ising partition function was presented (see also [12–16] for related work). Further, in [17] it was proven that computing the partition function of the Potts model is BQP–complete (see also [18, 19]). BQP stands for bounded–error quantum polynomial time, and, colloquially speaking, is the class of decision problems that can be efficiently approximated by a quantum computer, and the hardest problems in this class are called BQP–complete. This situation contrasts with that of a different class of classical spin models, namely lattice gauge theories with gauge group $\mathbb{Z}_2$ [20], for which, to the best of our knowledge, no results are known concerning their quantum computational complexity. These are models with "Ising variables" (i.e. classical degrees of freedom with two states) but which nonetheless exhibit local symmetries [21, 22].

In this paper we tackle the question of the quantum computational complexity both of several paradigmatic classical spin models as well as of a $\mathbb{Z}_2$ lattice gauge theory. Our approach builds upon a mapping between partition functions and quantum circuits introduced in [23]. In that work, this mapping is exploited to show, among others, that estimating the partition function of the six vertex model and of Ising–type models is BQP–complete. Here we revisit this approach and extend the mapping to standard Ising models, Potts models and to $\mathbb{Z}_2$ lattice gauge theories. Based on that, we provide efficient quantum algorithms to estimate (with polynomial accuracy) the partition function of the six vertex model on a 2D square lattice, the Ising model with magnetic fields on a planar graph, the Potts model on a quasi 2D square lattice, and a 3D lattice gauge theory with gauge group $\mathbb{Z}_2$. Moreover, we show that computing the partition functions of these models is BQP–complete, that is, it is as hard as simulating arbitrary quantum computation. Therefore, in this work we put paradigmatic classical spin models and $\mathbb{Z}_2$ lattice gauge theories on an equal footing as far as their quantum computational complexity is concerned.

However, a word of caution is needed here: our results are valid mostly for a *complex* parameter regime of the models. This means that we can prove the complexity results only if the coupling strengths of these models have certain imaginary values (this problem is also encountered in [17, 23]). Note that although such complex parameters do not correspond to physical models, the partition function with complex arguments is commonly studied, e.g., in the context of evaluating the Tutte polynomial or finding (complex) zeros of $\mathcal{Z}$ to identify phase transition points [24]. We also want to stress that our results rely crucially on the fact that an *additive* approximation of the partition function is obtained (in contrast with a multiplicative approximation or an exact calculation), which, roughly speaking, means that the desired quantity is approximated with polynomial accuracy.

To summarize, the main results of this work are the following.

Statement of results. *Consider the partition function $\mathcal{Z}$ of the following classical spin models*

(i) *the six vertex model defined on a rectangular grid*

(ii) *the Ising model with magnetic fields defined on a planar graph,*

(iii) *the three–level Potts model on a quasi 2D square lattice with certain boundary conditions, and*

(iv) *the $\mathbb{Z}_2$ lattice gauge theory on a 3D square lattice,*

defined on a certain complex parameter regime, that is, the value of coupling strength J is, for example, $e^{\beta J} = i$. Furthermore, consider that there are certain values of the coupling strengths which appear together (i.e. certain sets of neighboring spins whose interaction takes a specific value). Then we provide efficient quantum algorithms to

approximate the partition function $\mathcal{Z}$ of these models with polynomial accuracy. Moreover, we show that estimating these partition functions is BQP–complete, that is, it is as hard as simulating arbitrary quantum computation.

Finally, as an extension of our results, we show that, if the Ising model considered above is defined on a lattice with periodic boundary conditions, then estimating its partition function with polynomial accuracy is DQC1–hard. This is the representative class of a scheme for quantum computation called the 'one clean qubit model', where all qubits but the first one are initialized in a totally mixed state [25].

This paper is structured as follows. In Sec. II we give a background on classical spin models, as well as on some notions of complexity of classical spin models. Then we review how to define BQP–complete problems as an estimation of a unitary matrix element (Sec. III). In Sec. IV we show how to relate partition functions of classical spin models with spin circuits, based on [23] and extended here. The main results of this work are presented in Sec. V, where we show the BQP–completeness of the six vertex model, the Ising model, the Potts model, and of the 3D lattice gauge theory with gauge group $\mathbb{Z}_2$ with certain conditions. In Sec. VI we present an extension of the results related to the one–clean–qubit model. Finally, we present our conclusions in Sec. VII.

II. CLASSICAL SPIN MODELS

In this section we will present some general considerations about classical spin models as well as some facts concerning their computational complexity.

A. General background

Classical spin models have proven successful to model magnetism, where they capture interesting physics such as critical phenomena despite their simplicity. More generally, classical spin models can serve as toy models for complex systems. For example, Ising models have been used to model neural networks (see Hopfield networks), or spin glasses (see, e.g., [5]).

Let us now define what is understood by a classical spin model. Common to all of them are the following ingredients:

(i) A degree of freedom represented by a classical spin which may take on a set of values: $s \in \{0, 1, ..., q - 1\}$. This is a q–level system.

(ii) A lattice, or more generally an arbitrary graph G, to which the classical spins are associated. They can sit at the vertices, edges or faces of the graph; the idea is that the graph encodes the interaction pattern of the model. The complexity of the model is affected by the lattice or graph on which it is defined, as we will see below.

(iii) An energy function $H(\mathbf{s})$ depending on a given spin configuration and the coupling strengths representing the types of interactions of the model: nearest–neighbor, many–body interactions, magnetic fields, etc.

(iv) A partition function $\mathcal{Z}$ which is obtained by summing over the Boltzmann weights of all spin configurations, $\mathcal{Z} = \sum_{\mathbf{s}} e^{-\beta H(\mathbf{s})}$.

From this common structure, several different families of models can be distinguished. One of the most relevant criteria is whether the model exhibits global or local symmetries (if any). We shall refer to the former as standard statistical models and to the latter as lattice gauge theories. This distinction of symmetry has profound consequences in the physics of the models. It is also related to their range of applicability: standard statistical models appear naturally in descriptions of classes of condensed matter systems and lattice gauge theories originated in the study of the fundamental interactions in nature and elementary particles.

Dimensionality is another key distinction which determines the complexity of the models. However, note that in order to have a well–defined notion of dimension for a graph G, this must be embedded in a smooth manifold of dimension D.

Standard statistical models can be divided into two big families depending on where the interactions on the graph G take place: vertex models and edge models. Vertex models were introduced to describe ice–type models, crystals with hydrogen bonding or ferroelectrics [4]. Edge models were introduced to explain phase transitions in materials with elementary magnetic moments [26, 27].

A vertex model consists of classical spins, namely q–level particles $s_e \in \{0, 1, \ldots, q-1\}$, which are placed on the *edges* of the lattice, and (typically many–body) interactions take place on the vertices. In the case of a (tilted) 2D lattice, one deals with four–body interactions between neighboring particles, and each of the spins participates in only two interactions. The Hamiltonian of such a system is given by

$$H = \sum_{a \in V} h^a(s_i, s_j, s_k, s_l), \qquad (1)$$

where $h^a(s_i, s_j, s_k, s_l)$ is a (local) four–body interaction term between the spins s_i, s_j, s_k, s_l sitting at the edges incident to vertex a. We denote the Boltzmann weight associated with this local energy as

$$w^a(s_i, s_j, s_k, s_l) := e^{-\beta h^a(s_i, s_j, s_k, s_l)}. \qquad (2)$$

The partition function is obtained by multiplying all local Boltzmann weights, and summing these over all spin configurations $\mathbf{s}$,

$$\mathcal{Z}_{\text{vm}} = \sum_{\mathbf{s}} \prod_a w^a(s_i, s_j, s_k, s_l). \qquad (3)$$

In contrast to vertex models, in edge models the classical spins sit at the vertices of the graph, also taking q possible states, $s_i \in \{0, \ldots, q-1\}$, and interactions take place along the edges. Consider, thus, a q–state edge model on an $n \times m$ square lattice with an edge–dependent energy function $h^e(s_i, s_j)$. Let

$$w^e(s_i, s_j) := e^{-\beta h^e(s_i, s_j)} \qquad (4)$$

denote the corresponding Boltzmann weight. Then the partition function is given by $\mathcal{Z} = \sum_{\mathbf{s}} \prod_{e=ij} w^e(s_i, s_j)$.

Concerning Lattice Gauge Theories (LGTs), the most relevant criterion to classify them is whether the internal gauge group $\mathcal{G}$ is Abelian (discrete like $\mathcal{G} = \mathbb{Z}_q$, or continuous $\mathcal{G} = U(1)$), or non–Abelian (discrete such as a permutation group $\mathcal{G} = S_3$, or continuous such as $\mathcal{G} = SU(N)$). We refer the reader to [20] for an introduction to these models. In this work we will focus on $\mathbb{Z}_2$ LGTs, and we will be in the following features: they are models whose classical spins can take two values $s_e \in \{0, 1\}$, they sit at the edges of a d–dimensional square lattice, and they interact along the faces of this lattice. More precisely, the interaction of spins s_i, s_j, s_k, s_l at the boundary of face f, ∂f, has the form

$$h_f(s_i, s_j, s_k, s_l) = -J_f \delta(s_i + s_j + s_k + s_l), \qquad (5)$$

where the sums are performed modulo 2 throughout this section, and $\delta(0) = 1$ and it is 0 otherwise. The Hamiltonian is then obtained as a sum over interactions on every face:

$$H(\mathbf{s}) = -\sum_f h_f(\{s_e : e \in \partial f\}), \qquad (6)$$

where ∂f denotes the boundary of face f.

These models exhibit $\mathbb{Z}_2$ gauge symmetry; more precisely, its Hamiltonian is invariant under $\mathbb{Z}_2$ operations around any vertex, $g_v = \prod_{e \in \text{inc } v} X_e$, where $e \in \text{inc } v$ denotes all edges incident to vertex v, and X_e is a flip operator, $X_e : s \to s + 1$. One can use this symmetry to eliminate some degrees of freedom, a process usually referred to as 'gauge fixing'. A specific choice of this fixing is the 'temporal gauge', where all degrees of freedom in one particular direction (the one associated with time) are fixed. A restriction about gauge fixing that concerns us is the fact the edges whose variable has been fixed by the gauge cannot form a closed loop [28]. This fact will be important in our proof of the BQP–completeness of this model in Sec. V D.

B. Classical computational complexity of spin systems

In this section we will be interested in the classical computational complexity of the classical spin models presented in Sec. II A. Generally speaking, understanding

the properties of, say, the Ising model on some graph is a difficult task. This is reflected by the fact that the Ising and other models are associated with hard problems in computational complexity theory [4]. For concreteness we will focus in the following on the Ising model, but the considerations in this section have general relevance.

Most prominently, the Ising model is known to be associated with computational problems which are NP–complete; here NP stands for 'non-deterministic polynomial time'. The complexity class NP consists of all decision problems f (i.e. YES/NO questions) which have the property that, for every input x for which it is claimed that $f(x) =$ YES, there exists a 'short proof' that this is indeed the case, i.e. a proof which may be efficiently verified as a function of the size of the input. More precisely, for each problem $f \in$ NP it is required that there exists an efficiently computable function V (the verifier of the proof) such that:

> For every input x, one has $f(x) =$ 'YES' if and only if there exists a poly–size bit string ξ (the witness) satisfying $V(x, \xi) =$ 'YES'.

Colloquially speaking, NP problems have the property that, whenever a solution to the problem is *proposed* (e.g. by an untrusted third party), it is possible to efficiently *verify* whether this proposed solution is indeed correct. Note that in the definition of NP no mentioning is made of the difficulty of *finding* a solution; even though a problem has an efficient verifier, it is a priori not excluded that the time required to find a solution scales exponentially with the input size.

An archetypical NP problem related to the Ising model is the problem of deciding whether the ground state energy of $H_G(\mathbf{s})$ on a graph G (which constitutes the input of the problem) is below a certain value K. This problem is indeed in NP: if the ground state energy of $H(\mathbf{s})$ is smaller than K, then the ground state provides a witness which allows to efficiently verify this fact; the verifier function is nothing but the energy function $H_G(\mathbf{s})$.

Not only is the problem of determining the Ising ground state in NP, it is among the hardest problems in this complexity class. This is reflected by the fact that this problem is known to be NP–complete. This means that every problem in the class NP can be reduced, with only polynomial computational effort in the input size of the problem, to an instance of the Ising ground state problem. This implies, in particular, that the existence of an efficient algorithm for the Ising ground state problem would yield an efficient algorithm for all problems in NP. The NP–completeness of the Ising model thus points to an intrinsic computational difficulty of this simple system.

There are several variants of the Ising ground state problem which are known to be NP–complete. We mention two of them.

Theorem 1 *[4]* *The following problems are* NP–*complete:*

(i) *Given a graph G and an integer K, determine whether the ground state energy of $H(\mathbf{s}) = \sum_{e=ab} s_a s_b$ is smaller than K.*

(ii) *Given a planar [40] graph G and an integer K, determine whether the ground state energy of $H(\mathbf{s}) = \sum_{e=ab} s_a s_b + \sum_a s_a$ is smaller than K.*

We remark that, in the second of these problems, the presence of the external fields ($h_a \equiv -1$) is crucial to obtain NP–completeness. Indeed, it is known that the ground state energy, as well as the partition function, of the Ising model on an arbitrary planar graph without external fields can be efficiently computed. We also note that the quantum computational complexity of the Ising model, as will be discussed in Sec. V B, will involve Ising models on planar graphs in the presence of magnetic fields.

The NP–completeness of the above ground state problems has strong implications for the evaluation of the corresponding partition functions. First, once the partition function of a model can be evaluated efficiently, also the ground state energy of the model can be efficiently determined: the evaluation of the partition function is 'at least as hard' as the evaluation of the ground state energy. Consequently, for the NP–complete Ising models, the evaluation of their partition function is NP–hard, i.e. at least as hard as any problem in NP. Note, however, that the evaluation of the partition function does not belong to the class NP, as it is not a decision problem but rather a counting problem. The relevant complexity class in this case is #P ('sharp-P'). Given an efficiently computable decision problem g (i.e. $g \in$ P), the problem of determining how many inputs yields the answer 'YES', represented by the number $\#g = |\{x : g(x) = \text{'YES'}\}|$, defines the complexity class #P.

Since the ground state problems of the Ising models in Theorem 1 are NP–complete, it can be shown that computing the corresponding partition functions are #P–complete problems: every problem in #P can be reduced, with polynomial computational effort, to the evaluation of the partition function of such an Ising model on some graph. This is formulated in the following result:

Theorem 2 *[4]* *The following problems are* #P–*complete:*

(i) *Given a graph G and $\lambda = e^{-\beta}$, determine the partition function $\mathcal{Z}(\lambda)$ of the Ising model on G with energy $H(\mathbf{s}) = \sum_{e=ab} s_a s_b$.*

(ii) *Given a planar graph G and $\lambda = e^{-\beta}$, determine the partition function $\mathcal{Z}(\lambda)$ of the Ising model on G with $H(\mathbf{s}) = \sum_{e=ab} s_a s_b + \sum_a s_a$.*

III. UNITARY MATRIX ELEMENTS AND BQP–COMPLETENESS

The goal of this paper is to relate the evaluation of partition functions to problems which are complete for *quan-*

tum complexity classes. The main complexity class which will be considered is 'bounded-error quantum polynomial time' (BQP), representing the class of decision problems which can be solved efficiently on a quantum computer. The route we will take to prove BQP–competeness of certain partition function problems will be to start from a standard complete problem for BQP and then to relate these problems to the approximation of partition functions. The standard BQP–complete problem in question involves estimating matrix elements of unitary quantum circuits, which we briefly discuss here.

Consider a quantum circuit U acting on n qubits, which is composed of poly(n) gates acting each on, say, at most two qubits. Let $\{|0\rangle, |1\rangle\}$ denote the single–qubit computational basis. Then there exists a well known technique to estimate the matrix element $\langle 0|^{\otimes n} U |0\rangle^{\otimes n}$ in poly–time on a quantum computer, using the 'Hadamard test' (see Fig. 1 and its caption for a brief a explanation— we refer to the literature, e.g. [18, 19, 29, 30], for further explanations). More precisely, for any approximation scale ϵ which scales at most inverse polynomially with n, the Hadamard test returns a complex number c which satisfies

$$|c - \langle 0|^{\otimes n} U |0\rangle^{\otimes n}| \leq \epsilon, \qquad (7)$$

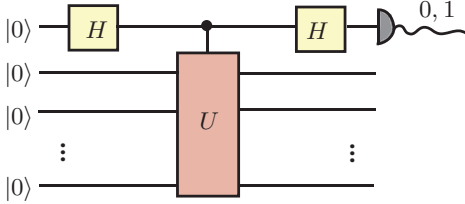with a success probability that is exponentially (in n) close to 1.

FIG. 1: The Hadamard test. This is performed with a quantum circuit where the first qubit is transformed with a Hadamard gate, then the unitary U is applied to rest of the qubits conditional on the state of the first qubit, and then a Hadamard gate is applied to the first qubit again. Finally, this qubit is measured in the σ_z basis. From the probability to obtain 0 and 1, p_0 and p_1 respectively, one can estimate the real part of c (denoted $\text{Re}(c)$), as they are related by $p_0 = [1 + \text{Re}(c)]/2$ and $p_1 = [1 - \text{Re}(c)]/2$. To estimate the complex part, the circuit is modified to include a phase gate $P = \text{diag}(1, i)$ after the first Hadamard gate and before the controlled–U gate. The probabilities to measure 0 and 1 are then related to the imaginary part of c (denoted $\text{Im}(c)$) as $\tilde{p}_0 = [1 - \text{Im}(c)]/2$ and $\tilde{p}_1 = [1 + \text{Im}(c)]/2$ (see also [18, 19, 29, 30]).

Moreover, estimating the above matrix element problem is BQP–hard, i.e. every decision problem that can be solved efficiently with a quantum computer can be reduced, with polynomial (classical) computational effort, to the estimation of such a matrix element with the aforementioned accuracy ϵ. Without loss of generality we

can restrict all operations to act on nearest–neighboring qubits, since the SWAP operation can be used to move distant qubits to nearest–neighbor positions (with linear overhead in the number of qubits). Thus, one has the following.

Theorem 3 *The following problem is BQP–hard:*

Consider an n–qubit quantum circuit U consisting of a polynomial number of two–qubit gates acting on nearest–neighbor qubits. Then provide a number c such that

$$|c - \langle 0|^{\otimes n} U |0\rangle^{\otimes n}| \leq \frac{1}{poly(n)} \qquad (8)$$

holds with a probability which is exponentially (in n) close to 1.

We provide a few remarks:

(i) One may adapt the formulation of Theorem 3 in a straightforward way to arrive at a BQP–complete decision problem (i.e. a problem that is both BQP–hard and in BQP). To do so, one considers circuits U for which it is *promised* that $|\langle 0|^{\otimes n} U |0\rangle^{\otimes n}|$ is either $\leq 1/3$ or $\geq 2/3$, and the goal is to decide which of these two cases holds.

(ii) BQP–hardness of the matrix element problem in Theorem 3 is maintained if one considers quantities of the form $\langle \psi | U | \psi' \rangle$, where $|\psi\rangle$ and $|\psi'\rangle$ are *fixed* complete product states, instead of $\langle 0|^{\otimes n} U |0\rangle^{\otimes n}$. This is because instances of the former matrix element problem can easily be reduced to instances of the latter. This property will be used in Secs. V A, V B and V C.

(iii) BQP–hardness is maintained when the circuit U is restricted to be composed of gates from a strongly universal elementary gate set. An elementary gate S consisting of gates acting on at most two qubits is said to be strongly universal if every two–qubit unitary operation can be approximated with arbitrary accuracy by products of elements from S. Further, BQP–hardness is also maintained if, instead of considering strongly universal unitary gate sets, gate sets are considered that are *encoded* universal for quantum computation, for a suitable notion of encoded universality. This will be important for our proofs in Secs. V A, V C and V D.

IV. MAPPINGS BETWEEN CLASSICAL LATTICE MODELS AND QUANTUM CIRCUITS

In this section we review the mappings between classical lattice models and quantum circuits (introduced and used in [23]), and we will extend them to standard Ising models, to Potts models and to $\mathbb{Z}_2$ LGTs. The mappings will allow us to interpret the partition function

of the classical model as a quantum expectation value. More precisely, consider a circuit $\mathcal{C}$ consisting of (unitary) quantum gates. Then we will show that partition functions $\mathcal{Z}$ of vertex models, edge models and $\mathbb{Z}_2$ LGTs are related to matrix elements of certain quantum circuits $\mathcal{C}$ as

$$\mathcal{Z} = \kappa \langle L|\mathcal{C}|R\rangle, \tag{9}$$

where $\langle L|$ ($|R\rangle$) are product states determined by the left (right) boundary conditions of the classical spin model (see below), and κ is a constant depending on the size of the lattice, i.e. the number of classical spins.

A. Vertex models

We start by considering vertex models (see Sec. II A). Here we essentially follow the argument of [23]. For illustration purposes, we will concentrate on a tilted 2D square lattice. However, our mappings are not restricted to such lattices and are easily generalized to other (regular) lattices.

Our construction begins with the following observation. The local Boltzmann weights (2) associated to each interaction can be seen as rank–four tensors of dimension q, or, equivalently, as $q^2 \times q^2$ matrices by grouping the indices into left indices (i, j) and right indices (k, l). We take the latter approach to associate each of these matrices with a quantum gate acting on two q–level quantum states (see Fig. 2),

$$W^a := \sum_{s_i, s_j, s_k, s_l} w^a(s_i, s_j, s_k, s_l)|s_i, s_j\rangle\langle s_k, s_l|. \tag{10}$$

Note that the right indices (k, l) correspond to the input of the gate, while the left indices (i, j) represent the output. The state is thus processed from right to left, where gates corresponding to outermost right vertices are performed in the first place [41]. The corresponding quantum circuit $\mathcal{C}$ is given by m layers of nearest–neighbor two–qubit gates (see Fig. 2),

$$\mathcal{C} = \prod_a W^a. \tag{11}$$

This can be seen as the contraction of a tensor network, i.e. as a summation over joined indices. For translational invariant models, each of the layers corresponds to the transfer matrix [4] of the classical model.

Thus, generally speaking, we have mapped a product of interactions of the classical spin model (which is essentially a partition function) to a contraction of quantum gates (which is essentially a quantum circuit). Now we only need to show how to map the boundary spins. We consider an $n \times m$ lattice with fixed boundary conditions, namely a lattice whose spins at the left and right boundary are fixed in some arbitrary configuration

$L = (s_1^L, \ldots, s_n^L)$ and $R = (s_1^R, \ldots, s_n^R)$, respectively. Using the spin states as computational basis states, we map these to two n–particle quantum states:

$$\begin{aligned} \langle L| &= \langle s_1^L|\ldots\langle s_n^L|, \\ |R\rangle &= |s_1^R\rangle\ldots|s_n^R\rangle. \end{aligned} \tag{12}$$

where we omit the tensor product symbol throughout this paper. Note that, since the qubits are processed from right to left, the state $|R\rangle$ serves as input for the circuit, while $|L\rangle$ constitutes the readout basis state.

It is now straightforward to see that the overlap of the resulting state $\mathcal{C}|R\rangle$ with the product state $\langle L|$ is exactly the partition function of the classical vertex model,

$$\mathcal{Z}_{\text{vm}}^{L,R} = \langle L|\mathcal{C}|R\rangle. \tag{13}$$

This concludes the mapping between matrix elements of quantum circuits and partition functions of classical spin models.
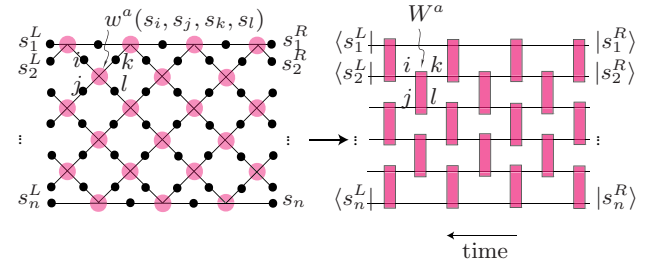

FIG. 2: (Left) In a vertex model, particles (black dots) sit at the edges and interactions (pale red dots) take place in the vertices. (Right) This model is mapped to a quantum circuit, where each particle becomes a qubit, and each interaction a two–qubit gate.

Now we make some remarks concerning this mapping.

(i) *Complex couplings.* Note that the quantum gates are specified by the parameters of the classical model, namely by the Boltzmann weights of the local interactions. It follows that the gates W^a (Eq. (10)) are unitary only in certain parameter regimes of the interaction w^a of the classical spin model. This will lead to the requirement of complex parameters in our proof of Sec. V A.

(ii) *Open and periodic boundary conditions.* This mapping can be easily extended to open boundary conditions, i.e. to systems where the left and right spins are 'free' and thus fully summed out in the partition function. This is achieved by replacing the left and right states $|L\rangle$ and $|R\rangle$ by the state $|+\rangle^{\otimes n}$, where $|+\rangle = q^{-1/2}\sum_{i=0}^q |i\rangle$ is a superposition over all q single spin states. This gives rise to the identity

$$\mathcal{Z}_{\text{vm}}^{\text{OBC}} = q^n\langle +|^{\otimes n}\mathcal{C}|+\rangle^{\otimes n}. \tag{14}$$

Furthermore, periodic boundary conditions can also be taken into account by summing over the diagonal matrix elements, which results in

$$\mathcal{Z}_{\text{vm}}^{\text{PBC}} = \text{Tr}(\mathcal{C}). \tag{15}$$

(iii) *Other geometries.* One can also consider other geometries such as vertex models on a 2D tilted triangular lattice [31], where six–body interactions take place at the vertices and the Boltzmann weights can be arranged into $q^3 \times q^3$ matrices, corresponding to a quantum circuit with three–body quantum gates. One such model is the 32 vertex model [31]. Also 3D models, such as models on a tilted 3D square lattice, are of this type and can thus be mapped to quantum circuits. In this case, one deals with three–body gates acting on a 2D array of quantum particles.

B. Edge models

In the following we will present a mapping for edge models, also following [23]. Unlike vertex models, in edges models interactions take place at the edges, as explained in Sec. II A. For the mapping we will distinguish between interactions at horizontal or vertical edges. More precisely, we associate a $q \times q$ matrix to each horizontal edge e:

$$W_e^h := \sum_{s_i, s_j} w^e(s_i, s_j) |s_j\rangle\langle s_i| , \qquad (16)$$

and a $q^2 \times q^2$ *diagonal* matrix to each vertical edge e,

$$W_e^v := \sum_{s_i, s_j} w^e(s_i, s_j) |s_i, s_j\rangle\langle s_i, s_j| . \qquad (17)$$

The matrices W_e^h and W_e^v will be regarded as (possibly non–unitary) quantum gates acting on a single, respectively a pair, of q–level quantum systems. We now consider a 1D quantum system composed of n q–level systems and the quantum circuit $\mathcal{C}$ acting on this system as depicted in Fig. 3. The circuit $\mathcal{C}$ consists of alternating layers of operations associated with the horizontal and vertical edges of the 2D lattice. Each round of $\mathcal{C}$ associated with a layer of horizontal edges consists of a product of one–local operators W_e^h, whereas every round associated with a layer of vertical edges is a product of (commuting) two–local operations W_e^v. We define computational basis states $|L\rangle$ and $|R\rangle$ associated to the left and right boundary conditions, respectively, analogously to Eq. (12). With these definitions, one has the following correspondence:

$$\mathcal{Z}_{\mathrm{em}}^{L,R} = \langle L|\mathcal{C}|R\rangle . \qquad (18)$$

This equation is readily verified by employing the definitions of gates W_e^h and W_e^v.

We emphasize that the comments concerning the mapping for vertex models apply to this mapping with straightforward modifications: unitary gates lead to complex coupling strengths (see Sec. IV A remark (i)), and the mapping can be extended to open and periodic boundary conditions (see Sec. IV A remark (ii)). Now
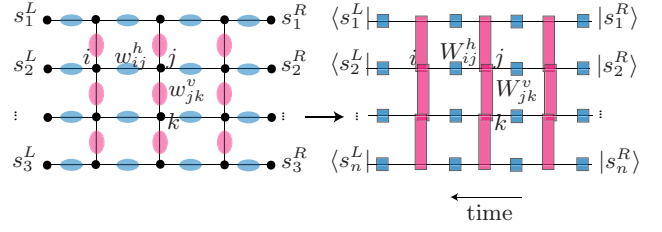

FIG. 3: (Left) In an edge model, particles (black dots) sit at the vertices and interactions (pale red and blue ellipses) take place along the edges. (Right) This model is mapped to a quantum circuit, where particles are mapped to qubits, interactions along the time direction become single–qubit gates, and interactions perpendicular to time become diagonal two–qubit gates.

we give some further modifications of the mapping for edge models that will be useful for the following sections.

(i) Consider that at site i in the lattice a local magnetic field is present. This is represented by an additional term $h_i(s_i)$ in the energy function and corresponding Boltzmann weight

$$w_i(s_i) = e^{-\beta h_i(s_i)} , \qquad (19)$$

with $s_i = 0, \ldots, q-1$. We associate to it the following diagonal $q \times q$ matrix

$$W_i := \sum_{s_i} w_i(s_i) |s_i\rangle\langle s_i| . \qquad (20)$$

Now a mapping to a quantum circuit $\mathcal{C}$ can be established in a similar fashion as above, with the distinction that each layer associated with a slice of vertical edges now consists of a product of the associated two–qubit gates W_e^v and the associated single–qubit gates W_i. Note that, as all such gates are diagonal operations, there is no problem regarding operator ordering. With this choice of $\mathcal{C}$, it can readily be verified that the associated partition function can be written as (18).

(ii) These mappings may be easily generalized to graphs other than the 2D lattice, also similarly as for vertex models (see Sec. IV A remark (iii)). In particular, below we will consider the following class of subgraphs of the 2D square lattice: a graph G is said to be a *planar circuit graph* if it can be obtained from an $n \times m$ rectangular grid (for some n and m) by *deleting* a subset of *vertical* edges and *contracting* a subset of *horizontal* edges. We call n the vertical dimension of G; note that this quantity is uniquely defined for every planar circuit graph. Similar as for the 2D square lattice, one can associate a quantum circuit $\mathcal{C}$ with every planar circuit graph; more precisely, such circuit acts n q–level systems, and one associates each horizontal and vertical edge e with

the gates W_e^h and W_e^v, respectively. Furthermore, local magnetic fields acting on the particles can also be easily incorporated by associating a gate W_i with each vertex i; see Fig. 4 for an example. This mapping will be relevant in Sec. V B.
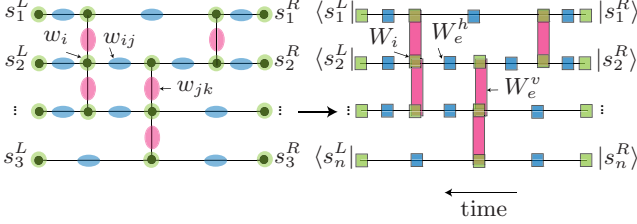

FIG. 4: (Left) Edge model with magnetic fields defined on a planar circuit graph. The latter is obtained from a rectangular grid by deleting some vertical edges and contracting some horizontal ones. (Right) This model is mapped to a quantum circuit: particles are mapped to qubits, and horizontal and vertical edge interactions are mapped to single–qubit (non–diagonal) and two–qubit diagonal gates, respectively, and local interactions (e.g. magnetic fields) are mapped to single–qubit diagonal gates.

In this paper we will be interested in two particular edge models: the Ising model and the Potts model. We now specialize the above discussion to the case of the 2D Ising model. We consider the Ising with magnetic fields defined on (sublattices of) a 2D square lattice. The interaction between spins s_i and s_j located at the endpoints of edge $e = (i, j)$ is given by

$$h_e(s_i, s_j) = -J_e\delta(s_i + s_j), \quad (21)$$

and the contribution of the magnetic field at site i is

$$h_i(s_i) = -h_i\delta(s_i). \quad (22)$$

Here the spin states s_i may take values 0 and 1, the sums are performed modulo 2 and as before $\delta(0) = 1$ and it is 0 otherwise. Further, J_e and h_i are constants which represent the strengths of the pairwise interaction and magnetic field, respectively. With the definitions (16), (17) and (20), we have

$$W_e^h = \begin{bmatrix} e^{\beta J_e} & 1 \\ 1 & e^{\beta J_e} \end{bmatrix}, \quad W_e^v = \text{diag}(e^{\beta J_e}, 1, 1, e^{\beta J_e}),$$
$$W_i = \begin{bmatrix} e^{\beta h_i} & 0 \\ 0 & 1 \end{bmatrix}. \quad (23)$$

Now we concentrate on the mapping for the Potts model. Given a graph G with vertex set V and edge set E, the Potts model [3] consists of q–level particles sitting at the vertices of G and interacting along the edges of G. Let u, v denote two such q–level particles $u, v \in \{0, 1, \ldots, q-1\}$, which interact along edge e. Then the Potts–type interaction is of the form

$$h^e(u, v) = -J_e\delta(u - v). \quad (24)$$

where $\delta(0) = 1$ and it is 0 otherwise. We shall later consider a more general form of this interaction:

$$h^e(u, v) = -J_{u=v}\delta(u - v) - J_{u \neq v}(1 - \delta(u - v)). \quad (25)$$

This amounts to a shift of the interaction energy which does not change the physics. Let $\mathbf{s}$ denote the spin state of all particles: $\mathbf{s} = (u, v, \ldots)$. Then the Hamiltonian of the Potts model is a sum of these two–local terms over all edges

$$H(\mathbf{s}) = \sum_{e \in E} h^e(u, v). \quad (26)$$

C. Lattice gauge theories

Now we focus on another family of models, namely $\mathbb{Z}_2$ LGTs (see Sec. II A), and we will introduce mappings for their partition functions.

We shall restrict the following discussion to a 3D $\mathbb{Z}_2$ LGT with the temporal gauge. As explained in Sec. II A, fixing this gauge is achieved by fixing all spins lying on edges with a specific direction of the lattice (the 'time' direction). However, the mapping can be generalized in a straightforward manner to 3D $\mathbb{Z}_2$ LGTs with another gauge fixing of the spins—we will return to this comment below and in Sec. V D. Because of the temporal gauge fixing, interactions in the time direction are two–body interactions, whereas those in the spatial direction (i.e. in faces without an edge in the time direction) remain four–body interactions as originally. To construct the mapping, we proceed similarly as above. We associate the Boltzmann weight of the two–body interaction at the temporal face

$$w_f^t(s_i, s_j) := e^{-\beta h_f(s_i, s_j)}, \quad (27)$$

with a single–qubit (non–diagonal) gate W_f^t,

$$W_f^t := \sum_{s_i, s_j} w_f^t(s_i, s_j)|s_j\rangle\langle s_i|. \quad (28)$$

Further, the Boltzmann weight of the four–body interaction at the spatial face

$$w_f^s(s_i, s_j, s_k, s_l) := e^{-\beta h_f(s_i, s_j, s_k, s_l)} \quad (29)$$

is mapped to a four–qubit diagonal gate W_f^s

$$W_f^s := \sum_{s_i, s_j, s_k, s_l} w_f^s(s_i, s_j, s_k, s_l) \times$$
$$|s_i, s_j, s_k, s_l\rangle\langle s_i, s_j, s_k, s_l|. \quad (30)$$

Thus, this maps the 3D $\mathbb{Z}_2$ LGT to a quantum circuit where a 2D array of qubits is processed in the time direction with single–qubit gates, and in the spatial direction with (diagonal) four–qubit gates (see Fig. 5). As before, it follows that the partition function $\mathcal{Z} = \sum_{\mathbf{s}} \prod_f w_f^s w_f^t$

is mapped to a quantum a circuit $\mathcal{C} = \prod_f W_f^s W_f^t$. Let L, R denote the left and right boundaries, respectively, as in Eq. (12). Then our mapping reads

$$\mathcal{Z}_{\mathrm{LGT}}^{L,R} = \langle L|\mathcal{C}|R\rangle. \tag{31}$$

Similarly as for vertex and edge models, we note that unitary gates will be translated to complex coupling strengths (as in Sec. IV A remark (i)), and one can obtain similar mappings for LGTs with open and periodic boundary conditions (see Sec. IV A remark (ii)). Next we make some further comments about this construction.

(i) The mapping can easily be extended to $\mathbb{Z}_2$ LGTs with other gauge fixings. As a matter of fact, we will use one of these mappings in Sec. V D. Since one deals with square lattices, one can always associate one dimension of the lattice to time. Then, generally, one fixes some spins in the time direction and some others in the space direction, the only restriction being the avoidance of closed loops (see the comment in Sec. II A and [28]). This introduces new type of interactions. For example, there can be a face in the space direction where three spins have been fixed by the gauge, and thus only one variable is left:

$$w_f(s_i) = e^{-\beta h_f(s_i)}. \tag{32}$$

Such interactions are mapped to single–qubit *diagonal* gate W_f^s:

$$W_f^s = \sum_{s_i} w_s(s_i)|s_i\rangle\langle s_i|. \tag{33}$$

Examples of these gates will be given in Sec. V D. Note, however, that the mapping does not need to be defined on all faces: for the BQP–completeness proof it suffices to specify the coupling strength on every face. In particular, we will set $J = 0$ on faces in the time direction where the temporal gauge is *not* fixed, and the interactions are not mapped to a gate in this case.

(ii) Notice that, due to the form of the interaction of this system (given by (5)), each gate is specified by only one parameter: $e^{\beta J}$. We will make repeated use of this fact in Sec. V D.

(iii) This mapping can be extended to $\mathbb{Z}_q$ LGTs (see [20] for an introduction of these models). In this case, each interaction can take q values, and they would translate to one– and four–*qudit* gates, where each qudit is a q–level quantum system.

(iv) More generally, the mapping can also be extended to $\mathbb{Z}_2$ LGTs defined on square lattices in d dimensions. The constructions is a generalization of the 3D case, where one has to select a translational invariant time direction out of the d dimensions,

and fix the temporal gauge. Since interactions also take place on the faces, time and space interactions are also mapped to one– and four–qubit gates, respectively. This results in a quantum circuit that processes a $(d-1)$ dimensional array of spins with single–qubit gates in the time direction, and with four–qubit gates in the space dimensions. Similar considerations apply to $\mathbb{Z}_q$ LGTs, with one– and four–qudit gates.

V. BQP–COMPLETENESS RESULTS

This section contains the central results of this paper: here we will provide efficient quantum algorithms to estimate the partition function of the six vertex model, the Ising model, the Potts model and the 3D $\mathbb{Z}_2$ LGT in a certain (complex) parameter regime, with polynomial accuracy. Moreover, we will show that approximating these partition functions is BQP–complete.

A. Six vertex model

Our goal is to prove that approximating the partition function $\mathcal{Z}$ of some vertex models in a certain (complex) parameter regimes is BQP–complete (see also [23]). To show that, we will make use of the mappings between vertex models and quantum circuits described in Sec. IV A.

We consider the $q = 2$ six vertex model (or: 'ice–type model') and the eight vertex model [4] on a (tilted) 2D square lattice. In the six vertex model, only 6 of the 16 possible spin configurations give rise to a non–zero Boltzmann weight. More precisely, W^a is a 4×4 matrix of the form

$$W^a = \begin{pmatrix} w_{00,00} & 0 & 0 & 0 \\ 0 & w_{01,01} & w_{01,10} & 0 \\ 0 & w_{10,01} & w_{10,10} & 0 \\ 0 & 0 & 0 & w_{11,11} \end{pmatrix}, \tag{34}$$

where we use w_{s_i,s_j,s_k,s_l} as a shorthand notation for $w(s_i, s_j, s_k, s_l)$ (see Eq. (10)). The eight vertex model [4] is obtained by additionally allowing the entries $w_{00,11}, w_{11,00}$ to be non–zero. We consider a parameter regime of the classical model where all matrices W^a are unitary. This gives rise to a unitary circuit $\mathcal{C}$ formed of two–qubit quantum gates. Notice that this generally corresponds to (non–physical) complex parameters for either coupling strengths J or the inverse temperature β as we pointed out in Sec. IV A remark (i). Finally, we assume that we have staggered left an right boundary conditions of the form $L = R = (0101\dots)$. Our result is the following.

Result 1 (BQP–completeness of the six vertex model) *Consider the six vertex model defined on a $n \times poly(n)$ rectangular grid with fixed boundary conditions. Further, consider that this is defined at inverse*
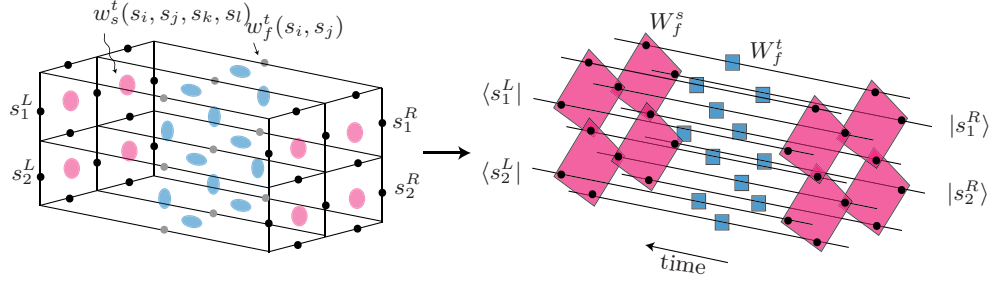
FIG. 5: (Left) In a 3D LGT, particles (black and gray dots) sit at the edges and interactions (pale red and blue ellipses) take place on the faces. Gray dots indicate particles whose state has been fixed by the gauge. (Right) This model is mapped to a quantum circuit, where interactions along the time direction become single–qubit gates (blue squares), and those perpendicular to it become four–qubit gates (pale red squares). Thus, a 2D array of qubits is processed by a circuit consisting of a sequence of single–qubit gates and diagonal four–qubit gates.

temperature β and with couplings strengths

$$
\begin{aligned}
w_{00,00} &= w_{11,11} = e^{i2t} \\
w_{01,01} &= w_{10,10} = \cos(2t) \\
w_{01,10} &= w_{10,01} = i\sin(2t)\,,
\end{aligned}
\tag{35}
$$

where t is a continuous parameter, and

$$
\begin{aligned}
w_{00,00} &= w_{11,11} = 1 \\
w_{01,01} &= w_{10,10} = w_{01,10} = -w_{10,01} = \tfrac{1}{\sqrt{2}}\,.
\end{aligned}
\tag{36}
$$

Let $\mathcal{Z}$ denote the partition function of this model. Then we provide efficient quantum algorithms to estimate $\mathcal{Z}$ with polynomial accuracy. We also show that the problem of approximating $\mathcal{Z}$ is BQP–complete.

Before starting the proof, we remark boldface symbols will denote encoded states and operators throughout this paper. To prove Result 1, we will show that any quantum computation can be reduced to the evaluation of the partition function of a six vertex model on a tilted 2D square lattice with staggered boundary conditions. We prove this statement in the following steps:

1. We show that quantum gates of the form (34) are computational universal for *encoded* quantum computation. To do so, we use the four–qubit encoding for $|\mathbf{0}\rangle$ given by Refs. [32, 33], which is of the form:

$$
|\mathbf{0}\rangle = \frac{1}{2}(|01\rangle - |10\rangle)^{\otimes 2}\,.
\tag{37}
$$

Note that $|\mathbf{1}\rangle$ can be prepared by means of the encoded universal circuit that we will show next.

Now we consider the exchange (or Heisenberg) interaction,

$$
H_{\mathrm{ex}} = \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z\,,
\tag{38}
$$

with corresponding two–qubit gates

$$
U = e^{itH_{\mathrm{ex}}}\,.
\tag{39}
$$

The Heisenberg interaction is (encoded) universal for quantum computation [32, 33]. In other words, by using gates of the form (39), one can prepare any quantum state $|\boldsymbol{\psi}\rangle = \mathcal{C}|\mathbf{0}\rangle$ in an encoded form. Gates of the form (39) can be generated with six vertex–type gates, i.e. of the form (34), by setting the non–zero entries specified in (35).

2. Now we show that the encoded initial state $|\mathbf{0}\rangle^{\otimes N}$ can be prepared from the state corresponding to staggered boundary conditions $|0101\ldots\rangle$. To this aim, we consider an operation V of the form (34) with the non–zero entries of Eq. (36). It is straightforward to check that $V|01\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, and hence

$$
|\mathbf{0}\rangle = V^{\otimes 2}|0101\rangle\,.
\tag{40}
$$

3. Finally, we observe that matrix elements of the form $\langle \mathbf{0}|^{\otimes n}\mathcal{C}|\mathbf{0}\rangle^{\otimes n}$ can be efficiently approximated by a quantum computer with polynomial accuracy, as long as $\mathcal{C}$ can be implemented efficiently. Since we are dealing with a poly–size quantum circuit consisting of two–qubit gates (as indicated in Eq. (34)), $\mathcal{C}$ can be implemented efficiently. The estimation of the matrix element is achieved by the Hadamard test, as pointed out in Sec. III. These overlaps are related to partition functions of the six vertex model in a certain (complex) parameter regime via (13), since all gates U, V involved are of the form (34), and thus correspond to Boltzmann weights of the six vertex model.

This concludes the proof of Result 1.

We make a few remarks concerning this construction.

(i) Note that the complex parameter regime of Eqs. (35) and (36) is due to the fact that these entries correspond to unitary gates, as noted in Sec. IV A remark (i).

It is worth mentioning that in [34] it is shown that universal quantum computation can be achieved

with real gates alone (i.e. gates with real entries). Thus, at first sight, it may seem that applying this method to our circuits would allow us to prove results for a real parameter regime of the classical spin models. However, we remark that the entries of our entries correspond to the Boltzmann weights of the interactions, which are not only real but also *positive*. The latter condition is not satisfied in [34].

(ii) We observe that universality is already obtained for a suitable discrete set of unitary gates $e^{itH_{ex}}$ [32, 33], which leads to a discrete set of Boltzmann weights in the corresponding six vertex model.

B. Ising model

Here we show that approximating the Ising partition function in the presence of an external magnetic field is a BQP–complete problem. More precisely, we find the following.

Result 2 (BQP–completeness of the Ising model)
Consider any planar circuit graph G. Let τ denote the number of horizontal edges in G and let n be its vertical dimension. Consider a classical Ising model at inverse temperature β defined on G, where on each site a constant (complex) magnetic field h_a is present satisfying $e^{\beta h_a} = e^{\frac{i\pi}{4}}$, and on each edge a constant (complex) coupling J_e is present satisfying $e^{\beta J_e} = i$. Let $\mathcal{Z}$ denote the partition function of the model with open boundary conditions. Then we provide efficient quantum algorithms to estimate

$$\frac{\mathcal{Z}}{\kappa}, \quad \kappa := 2^{\frac{\tau}{2}+n}, \tag{41}$$

with polynomial accuracy. We also show that the problem of estimating (41) with this accuracy is BQP–complete.

The proof will consist of several steps. Gates corresponding to this model are of the form (23); in particular, we consider the gates

$$\begin{aligned} W_h &:= \begin{bmatrix} i & 1 \\ 1 & i \end{bmatrix}, \quad W_v := \operatorname{diag}(i,1,1,i) \\ V &:= \begin{bmatrix} e^{i\pi/4} & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned} \tag{42}$$

To show that (41) can be approximated with polynomial accuracy in poly–time with a quantum computer, we use the mapping of an edge model in the presence of a local magnetic field (with open boundary conditions) to a quantum circuit $\mathcal{C}$ described in Sec. IV B. Letting n be the vertical dimension of G as in the statement of the result, the associated quantum circuit $\mathcal{C}$ is an n–qubit circuit composed of the gates W_h, W_v and V. In particular, we have

$$\mathcal{Z} = 2^n \langle +|^{\otimes n} \mathcal{C} |+\rangle^{\otimes n}, \tag{43}$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Note that, for the values of the magnetic fields and the couplings adopted in the statement of the result, the matrices W_v and V are unitary. Moreover, the matrix $\bar{W}_h := W_h/\sqrt{2}$ is unitary as well. Letting $\bar{\mathcal{C}}$ denote the unitary quantum circuit obtained by replacing every gate W_h by $\bar{W}_h$, we simply have $\bar{\mathcal{C}} = \mathcal{C}/2^{\frac{\tau}{2}}$. It follows that

$$\frac{\mathcal{Z}}{2^{\frac{\tau}{2}+n}} = \langle +|^{\otimes n} \bar{\mathcal{C}} |+\rangle^{\otimes n}, \tag{44}$$

where the right hand side now represents a matrix element of a poly–size, *unitary* quantum circuit. From the Hadamard test it follows that estimating (41) with polynomial accuracy is achievable in poly–time on a quantum computer.

Next we show that approximating (41) with polynomial accuracy is BQP–hard. This proceeds in the following steps:

1. Denote $T := V^{\frac{1}{2}} \bar{W}_h V^{\frac{1}{2}}$, where $V^{\frac{1}{2}} := \operatorname{diag}(e^{\frac{i\pi}{8}}, 1)$. We will need the following result:

Lemma 1 (Universality of Ising–type gate set)
Any poly–size n–qubit quantum circuit composed of two–qubit unitary gates can be approximated to accuracy ϵ (with respect to the operator norm) by a circuit composed of $\operatorname{poly}(n, \frac{1}{\epsilon})$ single–qubit gates T and two–qubit gates $T^{\otimes 2} W_v T^{\otimes 2}$, where every such two–qubit gate is restricted to act on nearest–neighboring qubits only. Moreover the latter circuit can be found in time $\operatorname{poly}(n, \frac{1}{\epsilon})$.

This Lemma is proved in Appendix A; here we continue the argument to prove Result 2.

2. Consider an arbitrary poly–size n–qubit circuit U composed of two–qubit unitary gates. It follows from the discussion in Sec. III that the problem of approximating general matrix elements $\langle +|^{\otimes n} U |+\rangle^{\otimes n}$ with polynomial accuracy is BQP–hard. We now write U as

$$U = [V^{\frac{1}{2}}]^{\otimes n} U' [V^{\frac{1}{2}}]^{\otimes n} \tag{45}$$

for some suitable U'. Note that U' is again a poly–size circuit, and can be found efficiently. We denote $A := [V^{\frac{1}{2}}]^{\otimes n}$, i.e. $U = AU'A$.

3. Due to Lemma 1, every poly–size circuit U' can be approximated with accuracy ϵ by a circuit U'' of size $\operatorname{poly}(n, 1/\epsilon)$ composed of T gates and nearest–neighbor $T^{\otimes 2} W_v T^{\otimes 2}$ gates, and U'' can be found efficiently. This implies that each matrix element $\langle +|^{\otimes n} U |+\rangle^{\otimes n}$, where U is any poly–size circuit as before, can be approximated with accuracy $1/\operatorname{poly}(n)$ by a matrix element of the form

$$\langle +|^{\otimes n} AU''A |+\rangle^{\otimes n}, \tag{46}$$

where U'' is a poly–size circuit composed of T gates and nearest–neighbor $T^{\otimes 2} W_v T^{\otimes 2}$ gates. Hence,

also the problem of approximating the matrix elements (46) with 1/poly accuracy is BQP–hard. Our goal is to show that any such matrix element coincides with a quantity $\mathcal{Z}/\kappa$ as considered in Result 2.

4. By definition, the gates T and $T^{\otimes 2}W_v T^{\otimes 2}$ contain square roots of the operation V. However, the operation $AU''A$ only contains integral powers of the gate V. To see this, first note that any circuit U'' of T and $T^{\otimes 2}W_v T^{\otimes 2}$ gates only contains $V^{\frac{1}{2}}$ gates at the left and right 'boundary' of the circuit. In the circuit $AU''A$, each $V^{\frac{1}{2}}$ gate at the boundary is multiplied with another $V^{\frac{1}{2}}$ gate due to the presence of the left and right boundary operator A. As a result, the operation $AU'A$ is a genuine circuit composed of W_v, $\bar{W}_h$ and V gates.

5. With any such circuit $AU''A$ we now associate a graph G in the following way. With each single–qubit gate $\bar{W}_h$ we associate a single horizontal edge, and with each two–qubit gate W_v we associate a vertical edge. The entire graph G associated with the quantum circuit is then obtained by simply 'gluing' together these edges in the natural way. An example is given in Fig. 4. Note that the graph is indeed a planar circuit graph, and that the vertical dimension of G is n. Moreover, consider an Ising model defined on G with parameters β, J_e and h_e as in Result 2, with open boundary conditions, and let $\mathcal{Z}$ denote the partition function of the model. Then $\mathcal{Z}$ can be expressed as a matrix element of the form (14), for some circuit $\mathcal{C}$ composed of W_h, W_v and V gates. It is now straightforward to verify that, up to a normalization stemming from the presence of $1/\sqrt{2}$ in the gates $\bar{W}_h$, the circuit $\mathcal{C}$ coincides with the circuit $AU''A$. More precisely, letting τ denote the number of horizontal edges in G, one has $\mathcal{C} = 2^{\frac{\tau}{2}} AU''A$. This shows that

$$\langle +|^{\otimes n} AU''A|+\rangle^{\otimes n} = \frac{\mathcal{Z}}{2^{\frac{\tau}{2}+n}}. \tag{47}$$

It follows that every matrix element of the form (46) coincides with an Ising partition function with parameters β, J_e and h_a as in Result 2, defined on the associated planar circuit graph G. This proves that the problem of estimating $\mathcal{Z}/2^{\frac{\tau}{2}+n}$ with polynomial accuracy is BQP–hard.

C. Potts model

In this section we show that approximating partition function of the three–level Potts model with complex parameters on a quasi 2D square lattice is BQP–complete. To be precise, we find the following.

Result 3 (BQP–completeness of the Potts model)
Consider the Potts model with three–level particles defined on a poly–size quasi 2D square lattice with fixed boundary conditions. Let β denote the inverse temperature and $J_{u=v}$ ($J_{u\neq v}$) the coupling strength when the two interacting particles spins u and v are (not) in the same state (see (25)). Consider this model defined in the following parameter regime

$$\begin{aligned}(e^{\beta J_{u=v}}, e^{\beta J_{u\neq v}}) \in \ & \{(1,0),(e^{i\pi/8},1),(-i,1),\\ & (1,1),(0,1),(\epsilon,1),\\ & ((\sqrt{2}\epsilon)^{-1},1),(-1,1)\}\end{aligned} \tag{48}$$

where ϵ is a polynomially small number, i.e. $\epsilon = \mathcal{O}(1/\mathrm{poly}(n))$. Moreover, consider that certain 'blocks' of these coupling strengths appear together (that is, there are certain local distributions of couplings). Let $\mathcal{Z}$ denote the partition function of this model. Then we provide efficient quantum algorithms to estimate $\mathcal{Z}$ with polynomial accuracy. We also show that estimating $\mathcal{Z}$ with this accuracy is BQP–complete.

To prove this result, we will make use of the idea of encoded universal quantum computation as in Sec. V A. We will first present the encoding of physical qubits into logical ones, and then we will construct a universal gate set at the logical level with Potts–type gates.

First of all we define an encoding. According to our mapping of Sec. IV B, a three–level quantum particle (a *qutrit*) is associated to each three–level classical particle. Let $\{|0\rangle, |1\rangle, |2\rangle\}$ denote the basis states of each qutrit. We use two of these qutrits (which we refer to as *physical* qutrits) to encode one *logical* qubit, whose states $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ are defined as

$$\begin{aligned}|\mathbf{0}\rangle &= |0\rangle|1\rangle,\\ |\mathbf{1}\rangle &= |1\rangle|2\rangle.\end{aligned} \tag{49}$$

We will refer to the first and the second physical qutrits as the 'upper' and the 'lower qutrits', respectively. Note that, with this encoding, the input state $|\mathbf{0}\rangle|\mathbf{0}\rangle\ldots|\mathbf{0}\rangle$ requires no preparation, since it can be fixed as an initial boundary condition, viz. $|R\rangle = |0\rangle|1\rangle\ldots|0\rangle|1\rangle$.

Now we proceed with the construction of the encoded universal gate set. We first observe that, due to the Potts interaction (25), the gates (16) and (17) contain only two different coefficients; for further reference, we denote them

$$(\mu, \nu) := (e^{\beta J_{u=v}}, e^{\beta J_{u\neq v}}). \tag{50}$$

We construct the encoded universal gate set as follows:

- The single–qubit identity

$$\boldsymbol{I_1} = \sum_{\boldsymbol{i,j}=0}^{1} \delta(\boldsymbol{u},\boldsymbol{v})|\boldsymbol{u}\rangle\langle\boldsymbol{v}|, \tag{51}$$

  is achieved by applying a two–qutrit gate (between the two physical qutrits that compose the logical qubit) with $(\mu, \nu) = (1, 1)$ (see Fig. 6).

- The phase gate

$$\boldsymbol{P}_{\pi/8} = |\boldsymbol{0}\rangle\langle\boldsymbol{0}| + e^{i\pi/8}|\boldsymbol{1}\rangle\langle\boldsymbol{1}| \qquad (52)$$

is achieved by applying a two–qutrit gate between an auxiliary qutrit in the state $|2\rangle$ and the lower qutrit of the logical qubit with $(\mu, \nu) = (e^{i\pi/8}, 1)$ (see Fig. 6).

- The Hadamard gate

$$\boldsymbol{H} = \frac{1}{\sqrt{2}} \sum_{\boldsymbol{u},\boldsymbol{v}=0}^{1} (-1)^{\boldsymbol{uv}}|\boldsymbol{v}\rangle\langle\boldsymbol{u}| \qquad (53)$$

is more involved and we refer the reader to Appendix B for the details.

- The two–qubit identity gate

$$\boldsymbol{I_2} = \sum_{\boldsymbol{u},\boldsymbol{v}=0}^{1} |\boldsymbol{uv}\rangle\langle\boldsymbol{uv}|, \qquad (54)$$

is trivially obtained by applying a two qutrit–gate between the two physical qutrits of the first logical qubit with $(\mu, \nu) = (1, 1)$, and doing the same for the other logical qubit (see Fig. 7).

- Finally, the phase gate between logical qubits

$$\boldsymbol{CZ} = \sum_{\boldsymbol{u},\boldsymbol{v}=0}^{1} (-1)^{\boldsymbol{uv}}|\boldsymbol{uv}\rangle\langle\boldsymbol{uv}| \qquad (55)$$

is achieved by applying a two qutrit–gate between the lower qutrit of the first logical qubit and the upper qutrit of the second logical qudit with $(\mu, \nu) = (-1, 1)$. We also need to apply the same gate between the lower qudit of the second logical qubit and an auxiliary particle in the state $|2\rangle$ (see Fig. 7).
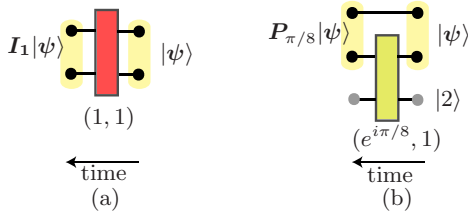

FIG. 6: Auxiliary qubits (i.e. fixed qubits) are depicted in gray, physical qubits in black, and logical qubits are highlighted in yellow. (a) Logical single–qubit identity $\boldsymbol{I_1}$. (b) Logical phase gate $\boldsymbol{P}_{\pi/8}$. Each gate is determined by the pair of numbers (μ, ν) (Eq. (50)) which are indicated next to it, and its color is just a guide to the eye to identify equal gates. Note that time runs in both figures from right to left.

In the construction presented above we need a constant supply of auxiliary qutrits, for which we envisage the following setup. We arrange the particles so that each
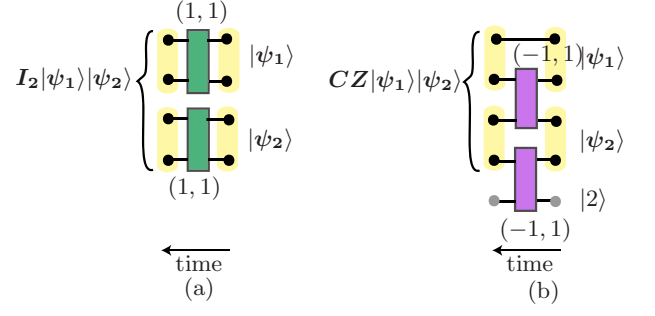

FIG. 7: (a) Logical two–qubit identity $\boldsymbol{I_2}$. (b) Logical controlled phase gate $\boldsymbol{CZ}$. See the caption of Fig. 6 for the meaning of the pair of numbers and the color associated to each gate.

physical qubit is in contact with four auxiliary qubits, as indicated in Fig. 8. Moreover, each physical qubit is propagated in time via a single–qubit gate at the physical level (that is, a gate of the form (16)) which is achieved with $(\mu, \nu) = (1, 0)$. In this way, the physical qubits are distributed on a 2D square lattice, which is surrounded (in front and on the back) by auxiliary qubits—we refer to this as a quasi 2D square lattice.

This proves that we can perform encoded universal quantum computation using qutrits interacting with Potts–type nearest–neighbor gates. From the discussion of Sec. III it follows that estimating $\langle\boldsymbol{0}|^{\otimes n}\boldsymbol{\mathcal{C}}|\boldsymbol{0}\rangle^{\otimes n} = \mathcal{Z}$ with polynomial accuracy is BQP–complete, where $\mathcal{Z}$ is the partition function specified in the statement of Result 3. This thus concludes the proof of Result 3.

We point out that our BQP–completeness result for the Potts model imposes constraints in the parameter regime as noted in Sec. IV B. We now give some further remarks regarding this proof.

(i) Note that to realize a gate in more than one step (like the Hadamard gate, see Appendix B) implies that one must fix the value of all those coupling strengths *together* in order to realize that gate in the quantum circuit. That is, the gate is only realized (and thus the complexity result is only achieved) if the classical model contains that 'block' of coupling strengths. These are thus constraints in the distribution of couplings imposed by the realization of gates.

(ii) We observe that the single–qubit identity at the physical level I_1 requires to set $\nu = 0$, which formally corresponds to setting $J_{u\neq v} = -\infty$. This unphysical regime can be avoided by letting $e^{\beta J_{u\neq v}}$ be a polynomially small number, that is $e^{\beta J_{u\neq v}} = \mathcal{O}(1/\mathrm{poly}(n))$ By the same argument as for the Hadamard gate (see Appendix B), the resulting state will be polynomially close to the ideal one, and thus the error within the accuracy of the computation.
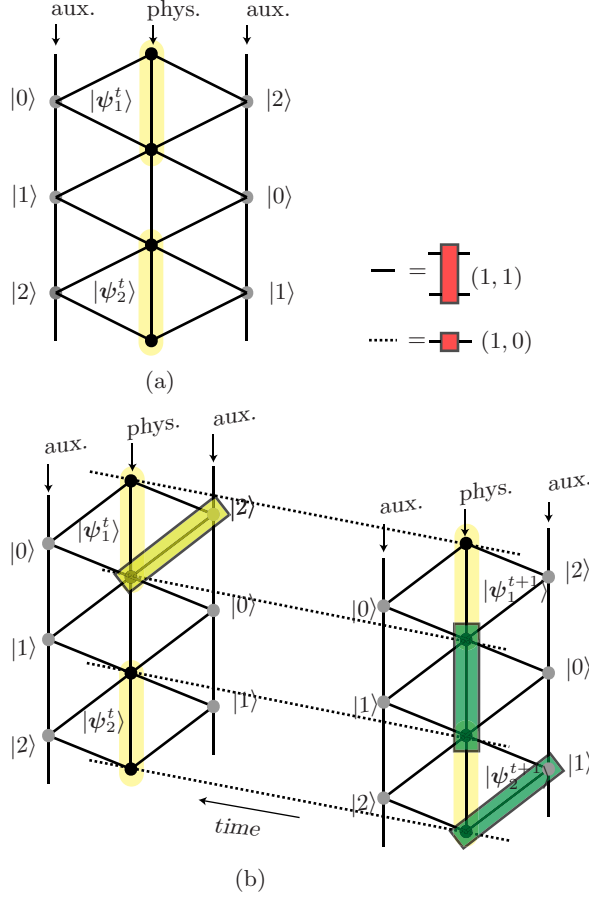
(a)

(b)

FIG. 8: Setup for a Potts model with the physical qutrits surrounded by auxiliary qutrits (i.e. qutrits whose value is fixed). Single–qutrit gates are applied in the time direction, and two–qutrit gates are applied in a fixed time slice. Solid and dashed lines stand for the two–qubit and single–qubit identities (at the physical level), respectively, as specified in the legend. (a) A time slice of the lattice at time t, where one can see the structure with two auxiliary qutrits connected to each physical qutrit. Each logical qutrit is composed of two physical qutrits. (b) Two time slices of the lattice, at times t and $t + 1$. The figure shows an example of a circuit, where a phase gate $\boldsymbol{P}_{\pi/8}$ is applied to $|\boldsymbol{\psi}_1^t\rangle$ and the gate $\boldsymbol{CZ}$ is applied to $|\boldsymbol{\psi}_1^{t+1}\rangle|\boldsymbol{\psi}_2^{t+1}\rangle$.

(iii) We see with our construction that the Potts model in a 1D array is not likely to be BQP–complete, whereas this model on a 2D setup (and with complex parameters) is BQP–complete. This is in agreement with the fact that the Potts model in 1D array or a tree–like structure is efficiently simulable classically [35].

(iv) Finally, this result can be generalized to Potts model with any q. In this case, the encoded states are still given by Eq. (49), and all gates are performed with the same procedure except for the Hadamard. For this gate, one adds filters for the $|3\rangle \ldots |q-1\rangle$ components on the upper and the lower

qudit right after the filters for the $|2\rangle$ and the $|0\rangle$ component of Fig. 10. That is, the number of filters scales linearly with q (since one requires $q-2$ filters for each qudit). Moreover, each physical qudit has to be connected to $2\lceil q/2 \rceil$ auxiliary particles, each fixed in a different state, namely $|0\rangle, \ldots, |q-1\rangle$. This amounts to a similar construction to that of Fig. 8 but where each physical qudit is connected to $\lceil q/2 \rceil$ auxiliary qudits to the left and to the right.

D. $\mathbb{Z}_2$ Lattice gauge theory

Now we turn to a different class of models, namely LGTs. Using the tools presented in Sec. IV C we will prove the following result.

Result 4 (BQP–completeness of the 3D $\mathbb{Z}_2$ LGT)
Consider a $\mathbb{Z}_2$ lattice gauge theory defined on a 3D rectangular lattice of size $(4x, 12y, 7z)$, where x, y and z are natural numbers, and with fixed boundary conditions. Let β denote the inverse temperature and J_f the coupling strength on its faces. Consider this model in the following complex parameter regime,

$$e^{\beta J_f} \in \left\{ 0, e^{i\xi}, \frac{1}{2}, \zeta \right\}, \qquad (56)$$

where ξ is a continuous parameter $\xi \in [0, 2\pi)$, and ζ is a polynomially small number, $\zeta = \mathcal{O}(1/poly(n))$. Moreover, consider that certain 'blocks' of couplings appear together, and that there is a certain gauge fixing. Let $\mathcal{Z}$ denote the partition function of this model. Then we provide efficient quantum algorithms to estimate

$$\frac{\mathcal{Z}}{\kappa}, \quad \kappa := 2^{\frac{xyz}{2}} \qquad (57)$$

with polynomial accuracy. We also show that the problem of approximating (57) is BQP–complete.

The proof of this result will proceed similarly as in the previous sections: we will construct an encoded universal gate set. We first define the following encoding of four physical qubits into one logical qubit:

$$\begin{aligned} |\boldsymbol{0}\rangle &= |0\rangle|0\rangle|0\rangle|0\rangle \\ |\boldsymbol{1}\rangle &= |1\rangle|1\rangle|1\rangle|1\rangle. \end{aligned} \qquad (58)$$

Note that preparing the input state $|\boldsymbol{0}\rangle$ is trivially achieved by fixing the physical qubits (which correspond to physical spins) in $|0\rangle|0\rangle|0\rangle|0\rangle$. In the following we show how to construct a general single–qubit unitary gate (at the logical level), and a specific two–qubit gate (also at the logical level), namely (the non–local part of) a controlled phase gate.

- First we express an arbitrary single–qubit rotation in its Euler decomposition,

$$\boldsymbol{U}(\gamma, \beta, \alpha) = \boldsymbol{R_z}(\gamma)\boldsymbol{H}\boldsymbol{R_z}(\beta)\boldsymbol{H}\boldsymbol{R_z}(\alpha). \qquad (59)$$

Thus, our goal is to generate arbitrary z–rotations and the Hadamard gate. The gate $\boldsymbol{R_z}(\xi)$ can be implemented by letting the logical qubit interact with a neighboring, auxiliary face which has all remaining qubits fixed to $|0\rangle$, and setting $e^{\beta J} = e^{i\xi}$ in this face (see Fig. 9).

The logical Hadamard gate $\boldsymbol{H}$ is implemented as a teleportation–based gate. We refer the reader to Appendix C for the details. We shall in fact apply a non–normalized version of this, namely $\tilde{\boldsymbol{H}} := \sqrt{2}\boldsymbol{H}$ (see below for a discussion of this normalization factor).

- To generate the logical controlled phase gate $\boldsymbol{CZ}$ we decompose it into single–qubit $\boldsymbol{R_z}$ rotations and a two–qubit gate:

$$\boldsymbol{CZ} = \boldsymbol{R_z^{(1)}}(-\frac{\pi}{2})\boldsymbol{R_z^{(2)}}(-\frac{\pi}{2})\,\mathrm{diag}(1,i,i,1)\,. \qquad (60)$$

The two–qubit gate $\mathrm{diag}(1,i,i,1)$ is implemented by letting the last two logical qubits interact via an auxiliary plaquette with $e^{\beta J} = i$ (see Fig. 9).
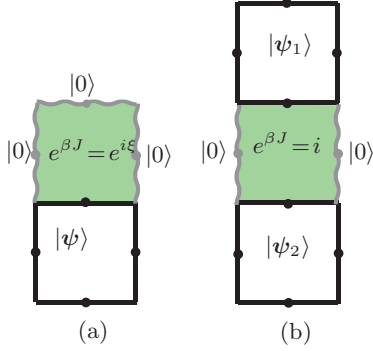

FIG. 9: The physical qubits composing the logical qubit are marked with thick, black lines, and wavy lines indicate qubits fixed by the gauge symmetry. Each gate is determined by $e^{\beta J}$. (a) The logical rotation around the z–axis, $\boldsymbol{R_z}(\xi)$ is obtained by letting the logical qubit interact with an auxiliary plaquette whose spins are all fixed to $|0\rangle$, and setting $e^{\beta J} = e^{i\xi}$ in this auxiliary plaquette. (b) The non–local part of $\boldsymbol{CZ}$, $\mathrm{diag}(1,i,i,1)$, is implemented by letting the two logical qubits interact via an auxiliary plaquette with $e^{\beta J} = i$.

Finally, we apply single–qubit identities at the physical level $I_1 := |0\rangle\langle0| + |1\rangle\langle1|$ on all physical qubits which belong to a logical qubit, unless otherwise specified. This gate is achieved by rescaling the interaction from $e^{\beta J_f}$ to $e^{\beta(J_f-1)}$, and then letting $e^{\beta(J_f-1)}$ tend to 0 polynomially fast (see Appendix C). We also set $J = 0$ on the faces whose interaction is not mapped to a quantum gate, which sets their corresponding Boltzmann weights to 1, thus not 'contributing' to the partition function. This is in accordance with the fact that these particles do not take part in the computation described by the quantum circuit.

Our construction of a circuit at the logical level differs from the general mapping presented in Sec. IV C in the following sense. The quantum circuit processes a *1D* array of logical qubits which are distributed along the x direction. These are transformed by four–qubit physical gates in the x direction (leading to logical single– and two–qubit gates), and by single–qubit physical gates in the z direction (which corresponds to time). The additional dimension (y direction) is required for the realization of the teleportation–based Hadamard gates, which transport the 1D array that stores the quantum information in the y direction.

Thus, we have constructed an encoded universal quantum circuit $\tilde{\mathcal{C}}$ with $\mathbb{Z}_2$–LGT–type gates, where $\tilde{\mathcal{C}}$ contains the non–normalized version of the Hadamard gates $\tilde{\boldsymbol{H}}$. Let $\mathcal{C}$ denote the unitary circuit containing the normalized Hadamard gates $\boldsymbol{H} = \hat{\boldsymbol{H}}/\sqrt{2}$. Then we have that

$$\frac{\mathcal{Z}}{2^{xyz/2}} = \langle\boldsymbol{0}|^{\otimes n}\boldsymbol{\mathcal{C}}|\boldsymbol{0}\rangle^{\otimes n}\,, \qquad (61)$$

where xyz is the number of times that the gate $\tilde{\boldsymbol{H}}$ is applied. From (61) and the discussion of Sec. III it follows that the estimating the partition function (57) with polynomial accuracy is BQP–complete. This concludes the proof of Result 4.

We emphasize that, as in the previous results, we require complex parameters due to the unitary gates. Also the remark (i) of Sec. V C applies here: performing a logical gate in several steps (like the Hadamard gate, see Appendix C) implies that a certain distribution of couplings must appear together in the classical model in order to prove our complexity result. Next we give some more comments concerning this result.

(i) Note that the single– and two–qubit identity gates $\boldsymbol{I_1}$ and $\boldsymbol{I_2}$ can be generated using the universal gate presented above. For example, $\boldsymbol{R_z}(0)\boldsymbol{H}\boldsymbol{R_z}(0)\boldsymbol{H}\boldsymbol{R_z}(0) = \boldsymbol{I_1}$ and $\boldsymbol{I_1^{(1)}}\boldsymbol{I_1^{(2)}} = \boldsymbol{I_2}$.

(ii) Result 4 is in contrast with the 2D $\mathbb{Z}_2$ LGT, whose complexity is 'trivial', i.e. it is in P when the temporal gauge is fixed. On the other hand, the 3D $\mathbb{Z}_2$ LGT can be mapped via a duality transformation to the 3D Ising model [20]. Thus, they share the same complexity in the parameter regime given by this transformation. We also observe that it was recently shown that computing the partition function of the 4D $\mathbb{Z}_2$ LGT in a real parameter regime is #P–complete [36, 37]. Concerning the quantum computational complexity of the 4D $\mathbb{Z}_2$ LGT (and, more generally, of any d $\mathbb{Z}_2$ LGT with $d > 3$), one can make the following trivial observation: any of these models can be "reduced" (i.e. become effectively equivalent) to the 3D $\mathbb{Z}_2$ LGT if the couplings in every face except those in a 3D volume are set to 0. Thus, our results imply that their complexity in this (trivial) parameter regime is BQP–complete. However, to the best of our knowledge, no quantum

computational results are known outside this trivial parameter regime.

VI. FURTHER RESULTS: ONE CLEAN QUBIT MODEL

Here we point out a connection between the results obtained on the Ising model in Sec. V B and a scheme for quantum computation called the 'one clean qubit model' [25]. In the latter, one considers a quantum computation where all qubits but the first one are initialized in the totally mixed state (and the first qubit is, say, in the state $|0\rangle$). To this initial state, an arbitrary poly–size quantum circuit may be applied, followed by a single–qubit measurement in the final stage of the computation. This one–clean–qubit model comprises a scheme that is believed to be weaker than the full power of quantum computers but stronger than classical computation (although these are unproved assertions). The corresponding complexity class of decision problems that can be solved efficiently with the one–clean–qubit scheme is called DQC1.

A standard problem that can be solved using the one clean qubit model is the problem of estimating normalized traces of unitary quantum circuits. Let U denote a poly–size n–qubit quantum circuit composed of, say, two–qubit gates. Then there exists an efficient quantum algorithm within the one clean qubit scheme which returns a number c that provides (with exponentially small probability of failure) an ϵ–approximation of the normalized trace $2^{-n}\text{Tr}(U)$ in poly(n) time, for every ϵ that scales at most inverse polynomially with n. The technique is a simple variant of the Hadamard test and we refer to the literature [25]. Moreover, the problem of estimating normalized traces of unitary quantum circuits is known to be DQC1–hard. In other words, this problem captures all problems that can be solved efficiently within the one clean qubit paradigm. It thus plays a similar role as the unitary matrix element problem for BQP.

Our results obtained in Sec. V B immediately lead to a complete problem for DQC1 involving Ising partition functions defined on graphs with *periodic boundary conditions*. We limit ourselves to a sketch of the argument. It follows from the discussion in Sec. V B that, for every poly–size quantum circuit U there exists an Ising model defined on a planar circuit graph G (which can be found efficiently), with couplings and temperature as in Result 2 and with open boundary conditions, such that $\mathcal{Z}/\kappa$ provides a 1/poly approximation of the matrix element $\langle +|^{\otimes n} U|+\rangle^{\otimes n}$. Now, instead of $|+\rangle^{\otimes n}$ we consider the matrix element $\langle s|U|s\rangle$ where $|s\rangle = |s_1 \dots s_n\rangle$ represents an arbitrary computational basis state. This matrix element now coincides with $\mathcal{Z}^s/\kappa$, where $\mathcal{Z}^s$ denotes the partition function of the same model (i.e. same graph, couplings and temperature), however considering boundary conditions where the left and right boundary spins are fixed in the same configuration s. Such a situation

is equivalent to considering a graph G' where each left boundary spin at the kth 'row' in the graph is *identified* with its corresponding right boundary spin, and the resulting spin is fixed in the state s_k, for all k. One thus arrives at an Ising model on a new graph G' which is obtained from G by enforcing *periodic boundary conditions*, and where one vertical slice of spins is fixed in the configuration s. Finally, consider the normalized trace of the matrix element U, given by $2^{-n}\sum_s \langle s|U|s\rangle$. Due to the above discussion, this normalized trace may be approximated with 1/poly accuracy by

$$\frac{1}{2^n \kappa} \sum_s \mathcal{Z}^s \ . \tag{62}$$

But as $\mathcal{Z}^s$ is the partition function on G' with one vertical slice of spins fixed in the configuration x, the sum $\sum_s \mathcal{Z}^s \equiv \mathcal{Z}'$ simply represents the partition function on G' where these spins are now fully summed out. The quantity $\mathcal{Z}'$ is hence the full–fledged partition function on G' of the Ising model with couplings and temperature as before, and without any fixed spins or boundary conditions.

We thus arrive at the following result: consider any planar circuit graph G. Let τ denote the number of horizontal edges in G and let n be its vertical dimension. Let G' be the graph obtained by enforcing periodic boundary conditions on G (as above). Consider a classical Ising model at inverse temperature β defined on G, where on each site a constant (complex) magnetic field h_a is present satisfying $e^{\beta h_a} = e^{\frac{i\pi}{4}}$, and on each edge a constant (complex) coupling J_e is present satisfying $e^{\beta J_e} = i$. Let $\mathcal{Z}'$ denote the partition function of the model. Then the problem of approximating

$$\frac{\mathcal{Z}'}{2^n \kappa}, \quad \kappa := 2^{\frac{\tau}{2}+n} \ , \tag{63}$$

with polynomial accuracy, is DQC1–hard.

VII. CONCLUSIONS

In this work we have shown that estimating the partition function of the six vertex model on a 2D square lattice, the 2D Ising model with magnetic fields on a planar graph, the Potts model on a quasi 2D square lattice, and the 3D $\mathbb{Z}_2$ LGT is BQP–complete. All these models must be defined in a (partially) complex parameter regime in order to prove the result. In all but the Ising model, we further require that certain blocks of coupling strengths appear together. Roughly speaking, that these problems are BQP–complete means that they are as hard as simulating arbitrary quantum computation. Because our proof is constructive, we have also provided the efficient quantum algorithms that estimate the partition functions of the above models. The proofs are based on a mapping from partition functions to quantum circuits introduced in [23] and extended here to the standard Ising

model, Potts model and to $\mathbb{Z}_2$ LGTs. In this sense, our work puts these different kinds of classical spin model on an equal footing as far as their quantum computational complexity is concerned.

It would be interesting to obtain quantum algorithms for computing such partition functions in a real parameter regime. At present we do not know whether our approach can be extended to prove such results. As we pointed in Sec. V A remark (i), the Boltzmann weights give rise not only to real but also to positive entries in the quantum gates. The latter seems to be a rather severe restriction in the pursuit of this goal.

Acknowledgements

Appendix A: Universality of the Ising–type gate set

The proof of Lemma 1 will use the following lemma.

Lemma 2 *Let $\epsilon > 0$ and define $K := \bar{W}_h V$. Up to a global phase, any two–qubit unitary operation can be approximated with accuracy ϵ (with respect to the operator norm) by a product of gates K and W_v i.e. these gates form a strongly universal gate set.*

Proof: Let $P := \mathrm{diag}(1, i)$ denote the phase gate, H the usual Hadamard gate, $H = \sum_{i,j=0,1}(-1)^{ij}|i\rangle\langle j|$, and Z denote the standard Pauli σ_z gate. We will also denote the controlled phase gate $\mathrm{CZ} := \mathrm{diag}(1, 1, 1, -1)$. Then the following identities can easily be verified:

$$
\begin{aligned}
ZKZKZ(K^\dagger)^2 Z &\propto H \\
KZK^\dagger ZK^\dagger ZK &\propto P \,.
\end{aligned} \tag{A1}
$$

Now note that $W_v^2 \propto Z \otimes Z$. Thus Eqs. (A1) imply that

$$
\begin{aligned}
W_v^2 K_1 W_v^2 K_1 W_v^2 [K_1^\dagger]^2 W_v^2 &\propto H \otimes I \\
W_v^2 K_1^\dagger W_v^2 K_1 W_v^2 K_1 W_v^2 K_1^\dagger &\propto P \otimes I \,.
\end{aligned} \tag{A2}
$$

So far we have showed that the operations $H \otimes I$ and $P \otimes I$ can be written as a product of gates K, $K^\dagger$ and W_v; the same is easily seen to hold for $I \otimes H$ and $I \otimes P$. Consequently:

(i) As $\mathrm{CZ} \propto [P \otimes P]W_v$, the CZ gate can also be written as a product of K, $K^\dagger$ and W_v gates;

(ii) As $W_h^\dagger \propto HP^3H$, the gate $V = \bar{W}_h^\dagger K$ (regarded as a two–qubit operation acting nontrivially on either the first or second qubit) can be written as a product of K, $K^\dagger$ and W_v gates as well;

(iii) As the gate K does not have finite order, there does not exist any integer m such that $K^m = K^\dagger$. However, it is well known that for every $\delta > 0$ there exists an integer $m = \mathrm{poly}(1/\delta)$ such that the distance (in operator norm) between K^m and $K^\dagger$ is at most δ.

This shows that the gates H, V as well as the CZ gate can be approximated with accuracy ϵ by a product of $\mathrm{poly}(1/\epsilon)$ gates K and W_v. Moreover, it is known that the CZ, H and V gates generate a dense subgroup of $U(4)$ (up to global phases). This hence proves Lemma 2. $\square$

The proof of Lemma 1 is now obtained as follows. We simultaneously conjugate the gates K and W_v with the operation $V^{\frac{1}{2}}$ acting on each qubit, yielding

$$
\begin{aligned}
[V^{\frac{1}{2}}]K[V^{\frac{1}{2}}]^\dagger &= T \\
\left[V^{\frac{1}{2}} \otimes V^{\frac{1}{2}}\right] W_v [V^{\frac{1}{2}} \otimes V^{\frac{1}{2}}]^\dagger &= W_v \,.
\end{aligned} \tag{A3}
$$

As K and W_v generate a dense subgroup of $U(4)$ up to global phases due to Lemma 2, the same holds for T and W_v since the latter gates are obtained by conjugating the former with the same fixed local unitary operation. Finally, it follows that also the gates T and $T^{\otimes 2}W_v T^{\otimes 2}$ generate a dense subgroup of $U(4)$ up to global phases: indeed, $T^\dagger$ can be approximated with arbitrary accuracy by powers of T, such that $W_v = T^\dagger[T^{\otimes 2}W_v T^{\otimes 2}]T^\dagger$ can be approximated with arbitrary accuracy by products of T and $T^{\otimes 2}W_v T^{\otimes 2}$.

We have thus showed that every two–qubit operation can be approximated with arbitrary accuracy by products of T and $T^{\otimes 2}W_v T^{\otimes 2}$. The Solovay–Kitaev Theorem then guarantees fast convergence, i.e. every poly–size n–qubit circuit composed of two–qubit gates can be approximated with accuracy ϵ by a circuit of $\mathrm{poly}(1/\epsilon, n)$ gates T and $T^{\otimes 2}W_v T^{\otimes 2}$; moreover, the latter circuit can be found efficiently, i.e. in $\mathrm{poly}(1/\epsilon, n)$ time. Hence this proves the claim.

Appendix B: Hadamard rotation with Potts–type gates

In the following we show how to obtain a Hadamard gate with Potts–type gates. Consider a general state (defined at the logical level), $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are arbitrary, normalized coefficients, $|\alpha|^2 + |\beta|^2 = 1$. Our goal is to apply a Hadamard gate to this state, that is, to transform it to $|\psi\rangle := \alpha|+\rangle + \beta|-\rangle$, where

$$
|\pm\rangle := \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \,, \tag{B1}
$$

by analogy with the conventional definitions $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$.

To apply this gate, we first observe that a Hadamard rotation can be decomposed as

$$
H = R_z(3\pi/2)R_x(\pi/4)R_z(3\pi/2) \,. \tag{B2}
$$

Then these three gates can be achieved with the following sequence of Potts–type gates (see Fig. 10):

1. A two qutrit–gate between an auxiliary qutrit in the state $|2\rangle$ and the lower qutrit of the logical qubit with $(\mu, \nu) = (-i, 1)$, which results in the state $\alpha|0\rangle|1\rangle - i\beta|1\rangle|2\rangle$.

2. A single–qutrit gate on the upper qutrit with $(\mu, \nu) = (-i, 1)$, and then a single–qutrit gate on the second qutrit with $(\mu, \nu) = (1, 1)$, which results in the state $\alpha(-i|0\rangle + |1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle) - i\beta(|0\rangle - i|1\rangle + |2\rangle)(|0\rangle + |1\rangle + |2\rangle)$.

3. A two–qutrit gate between an auxiliary qutrit in $|2\rangle$ and the upper qutrit with $(\mu, \nu) = (0, 1)$, and the same gate between an auxiliary qutrit in $|1\rangle$ and the lower qubit, which results in the state $\alpha(-i|0\rangle + |1\rangle)(|1\rangle + |2\rangle) - i\beta(|0\rangle - i|1\rangle)(|1\rangle + |2\rangle)$.

4. A two qutrit gate between the upper and lower qutrit with $(\mu, \nu) = (0, 1)$, which yields the state $\alpha(-i|0\rangle|1\rangle - i|0\rangle|2\rangle + |1\rangle|2\rangle) - i\beta(|0\rangle|1\rangle + |0\rangle|2\rangle - i|1\rangle|2\rangle)$.

5. A two qutrit gate between an auxiliary qutrit in $|0\rangle$ and the upper qutrit with $(\mu, \nu) = (\epsilon, 1)$, and the same gate between an auxiliary qutrit in $|2\rangle$ and the lower qutrit. Then a two–qutrit gate between an auxiliary qutrit in $|1\rangle$ and the upper qutrit with $(\mu, \nu) = (1/(\epsilon\sqrt{2}), 1)$, and the same gate between an auxiliary qutrit in $|1\rangle$ and the lower qutrit. Up to terms of order $\mathcal{O}(\epsilon^2)$, the resulting state is $[\alpha(-i|0\rangle|1\rangle + |1\rangle|2\rangle) - i\beta(|0\rangle|1\rangle - i|1\rangle|2\rangle)]/\sqrt{2}$. See below for a discussion of the accuracy of the gate due to neglecting these higher order terms.

6. A two–qutrit gate between an auxiliary qutrit in $|0\rangle$ and the upper qutrit with $(i, 1)$, and another two–qutrit gate between an auxiliary qutrit in $|1\rangle$ and the upper qutrit. The resulting state is $[\alpha(|0\rangle|1\rangle + i|1\rangle|2\rangle) + \beta(|0\rangle|1\rangle - i|1\rangle|2\rangle)]/\sqrt{2}$.

7. Finally, a two–qutrit gate between an auxiliary qutrit in $|2\rangle$ and the lower qutrit with $(-i, 1)$, after which the state of the system is $[\alpha(|0\rangle|1\rangle + |1\rangle|2\rangle) + \beta(|0\rangle|1\rangle - |1\rangle|2\rangle)]/\sqrt{2} = \alpha(|\mathbf{0}\rangle + |\mathbf{1}\rangle)/\sqrt{2} + \beta(|\mathbf{0}\rangle - |\mathbf{1}\rangle)/\sqrt{2} = \boldsymbol{H}|\boldsymbol{\psi}\rangle$, as we wanted to show.

Note that, due to step 5, the desired gate is achieved up to an error of $\mathcal{O}(\epsilon^2)$, where we use e.g. the Jamiołkowski Fidelity F [38] as a measure for the gate fidelity. Making use of the distance measure between the imperfect operation and the ideal Hadamard gate, $D(\mathcal{E}, \mathcal{U}) = \sqrt{1 - F}$, together with the chaining inequality [38, 39], $D(\mathcal{E}_1 \circ \mathcal{E}_2, \mathcal{U}_1 \circ \mathcal{U}_2) \le D(\mathcal{E}_1, \mathcal{U}_1) + D(\mathcal{E}_2, \mathcal{U}_2)$, we conclude that the total distance after M applications of an imperfect operation of this kind in a quantum circuit is at most M times the distance of a single imperfect operation. That is, $\sqrt{1 - F_{\text{tot}}} \le M\sqrt{1 - F}$, where F_{tot} denotes the Jamiołkowski fidelity of the overall circuit containing M imperfect operations, each with Jamiołkowski fidelity F. Hence, for any circuit consisting of a polynomial number of gates, $M = \mathcal{O}(N)$, a polynomial accuracy in ϵ, that is $\epsilon = \mathcal{O}(1/\text{poly}(N))$, suffices to achieve a polynomial accuracy of the total circuit. Notice that this is sufficient to obtain a final approximation of the partition function with polynomial accuracy [42].
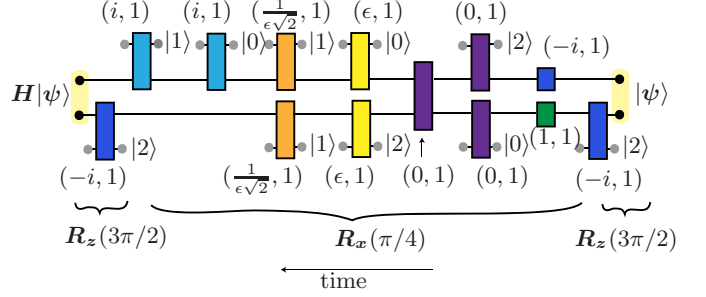

FIG. 10: The Hadamard rotation at the logical level, $\boldsymbol{H}$, is achieved by first performing a z–rotation $\boldsymbol{R_z}$, then an x–rotation $\boldsymbol{R_x}$ (which is itself composed of various gates) and finally another z–rotation $\boldsymbol{R_z}$. Most of the gates involve auxiliary qubits, whose input state is indicated on the right (since time runs from right to left). See the caption of Fig. 6 for the meaning of the pair of numbers and the color associated to each gate. See the text for the transformation of the state $|\boldsymbol{\psi}\rangle$ at each stage of the circuit.

Appendix C: Hadamard rotation with $\mathbb{Z}_2$ Lattice Gauge Theory–type gates

Here we show how to general single–qubit rotation of (59) with $\mathbb{Z}_2$ LGT–type gates. This operation includes $\boldsymbol{R_z}$ rotations, which we have shown how to perform in Sec. V D, and the non–normalized version of the logical Hadamard gate $\tilde{\boldsymbol{H}}$. We will implement the latter as a teleportation–based gate. Intuitively, the idea is the following. To apply $\tilde{\boldsymbol{H}}$ to the logical qubit $|\boldsymbol{\psi}\rangle$, we prepare two logical qubits next to it in the state $|\mathbf{0+}\rangle + |\mathbf{1-}\rangle$ (see (B1)). Then we apply a projection onto a Bell state $|\mathbf{00}\rangle + |\mathbf{11}\rangle$ between the qubit we want to teleport and the first of these two logical qubits. The third logical qubit is then left in the desired state, namely $\tilde{\boldsymbol{H}}|\boldsymbol{\psi}\rangle$.

More precisely, consider a general initial logical state $|\boldsymbol{\psi}\rangle = a|\mathbf{0}\rangle + b|\mathbf{1}\rangle$, where a and b are unknown, normalized coefficients $|a|^2 + |b|^2 = 1$. Then we transform this state into $\boldsymbol{R_z}(\pi/2)\tilde{\boldsymbol{H}}\boldsymbol{R_z}(\alpha)|\boldsymbol{\psi}\rangle$ by applying the following sequence of steps (see Fig. 11):

1. Single–qubit gates with $e^{\beta J} = 1$ to all physical qubits of the two logical qubits on the right. Each of these gates transforms the state of the physical qubits from $|0\rangle$ to $|0\rangle + |1\rangle =: \sqrt{2}|+\rangle$. Thus, this results in the state $|\boldsymbol{\psi}\rangle 16| + + + +\rangle^{\otimes 2}$.

2. The four–qubit gate with $e^{\beta J} = e^{i(\alpha+\pi/2)}$ on the top physical qubit of the first logical qubit. Also the four–qubit gate with $e^{\beta J} = 0$ inside the plaquette where the last two logical qubits are defined, and the four–qubit gates with $e^{\beta J} = 0$ on the physical qubits on top and on the right of the last two logical qubits (as indicated in the second step of Fig. 11). This results in the state $(a|\mathbf{0}\rangle + e^{i(\alpha+\pi)}b|\mathbf{1}\rangle)[|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle]^{\otimes 2}$.

3. The four–qubit gates with $e^{\beta J} = 0$ between the physical qubits on the right and on the bottom of the last two logical qubits (as indicated in the third step of Fig. 11). The resulting state is $(a|\mathbf{0}\rangle + e^{i(\alpha+\pi)}b|\mathbf{1}\rangle)[|\mathbf{0}\rangle + |\mathbf{1}\rangle]^{\otimes 2}$

4. The four–qubit gate with $e^{\beta J} = i$ applied on the top physical qubit of the second logical qubit. A four–qubit gate with $e^{\beta J} = 0$ between the physical qubit on the right of the second logical qubit and the physical on the right of it, which we refer to as the "middle qubit" (see fourth step of Fig. 11), which propagates the state of the first qubit to the middle one. Then the four–qubit gate with $e^{\beta J} = i$ between the middle qubit and the left physical qubit of the third logical qubit. The resulting state is $(a|\mathbf{0}\rangle + e^{i(\alpha+\pi)}b|\mathbf{1}\rangle)[|\mathbf{0}\rangle(|\mathbf{0}\rangle + i|\mathbf{1}\rangle) - |\mathbf{1}\rangle(|\mathbf{0}\rangle - i|\mathbf{1}\rangle)]$.

5. Finally, two concatenated four–qubit gates with $e^{\beta J} = 0$ between the first and the second logical qubit, which corresponds to the projection onto the Bell state $\langle\mathbf{0}|\langle\mathbf{0}| + \langle\mathbf{1}|\langle\mathbf{1}|$. We are interested in the state of the third logical qubit, since this contains the result of the teleportation. This state is $a(|\mathbf{0}\rangle + i|\mathbf{1}\rangle) + e^{i\alpha}b(|\mathbf{0}\rangle - i|\mathbf{1}\rangle)$, which equals

$$\boldsymbol{R_z}(\pi/2)\tilde{\boldsymbol{H}}\boldsymbol{R_z}(\alpha)|\boldsymbol{\psi}\rangle. \qquad (C1)$$

Thus, this sequence of gates applies essentially the first two logical gates of a general single qubit rotation of (59). The rotation $\boldsymbol{R_z}(\pi/2)$ appearing in (C1) can be compensated in the next rotation (marked as time step 8 in Fig. 12) by applying a four–qubit gate with $e^{i(\beta+\pi/2)}$ (instead of $e^{i(\beta+\pi)}$, which

would be the analogous case to the rotation of step 3, where $e^{i(\alpha+\pi)}$ was applied). This results in the state $\boldsymbol{R_z}(\beta)\tilde{\boldsymbol{H}}\boldsymbol{R_z}(\alpha)|\boldsymbol{\psi}\rangle$. Then a teleportation–based Hadamard gate $\tilde{\boldsymbol{H}}$ is applied with the same procedure as the one described above, and this gives rise to the state $\boldsymbol{R_z}(\pi/2)\tilde{\boldsymbol{H}}\boldsymbol{R_z}(\beta)\tilde{\boldsymbol{H}}\boldsymbol{R_z}(\alpha)$. The final rotation must correct for this phase, and the four–qubit gate at step 11 of Fig. 12 must have $e^{i(\gamma-\pi/2)}$ (instead of $e^{i\gamma}$). The overall sequence implements the desired general single qubit gate, $\boldsymbol{R_z}(\gamma)\tilde{\boldsymbol{H}}\boldsymbol{R_z}(\beta)\tilde{\boldsymbol{H}}\boldsymbol{R_z}(\alpha)|\boldsymbol{\psi}\rangle$.

Moreover, we apply single–qubit identities at the physical level $I_1 := |0\rangle\langle 0| + |1\rangle\langle 1|$ on all physical qubits which belong to a logical qubit unless otherwise specified, as mentioned in Sec. V D (yellow faces in the temporal direction in Fig. 11). This gate is achieved by first rescaling the face interaction energy (Eq. (5)) to $-(J_f - 1)\delta(s_i + s_j + s_k + s_l)$. According to (28) this gives rise to single qubit gate whose diagonal elements are 1 and the off–diagonal elements are $e^{\beta(J_f-1)}$. Then the gate is achieved by setting $e^{\beta(J_f-1)} = \zeta$, where ζ is a polynomially small number. By the same argument as for the Potts single–qubit identity (see Sec. V C remark (ii)), this will result in polynomial error at the end of the computation, which is within the accuracy of the result.

Note that the unnormalized gate $\tilde{\boldsymbol{H}}$ is applied once in every volume of 4 units in the x direction, 12 units in the y direction, and 7 units in the z direction. As mentioned in Sec. V D, the number of these blocks is what gives rise to the factor appearing in (57).

Since the general single qubit unitary gate involves a number of spins fixed by the gauge, it is important to verify that no closed loops of fixed spins are formed [28]. This is because the gauge fixing only yields an equivalent theory if no loops are formed, since, e.g., order parameters of the theory are defined as products of variables on such closed loops. To verify that no such loops are formed we project our 3D lattice into a 2D lattice along the time direction (see Fig. 12), where one can easily recognize that there is no closed path of edges fixed by the gauge.

[1] H. E. Stanley, *Introduction to Phase Transitions and Critical Phenomena* (Oxford University Press, 1971).
[2] D. P. DiVincenzo, Science **270**, 255 (1995).
[3] F. Y. Wu, Rev. Mod. Phys. **54**, 235 (1984).
[4] R. J. Baxter, *Exactly solvable models in statistical mechanics* (Academic Press Limited, San Diego, CA, 1982).
[5] M. Mézard, G. Parisi, and M. A. Virasoro, *Spin glass theory and beyond* (World scientific, Teaneck, NJ, USA, 1987).
[6] M. Schulz, *Statistical Physics and Economics: Concepts, Tools and Applications* (Springer, 2003).
[7] R. K. Pathria, *Statistical Mechanics* (Elsevier, Second edition, 1996).
[8] C. M. Papadimitriou, *Computational complexity* (Reading, Massachusetts: Addison-Wesley, 1995).
[9] L. Onsager, Phys. Rev. **65**, 117 (1944).
[10] P. W. Shor, in *Proceedings 35th Annual Symposium on the Foundation of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), p. 124.
[11] D. A. Lidar and O. Biham, Phys. Rev. E (1997).
[12] D. A. Lidar, New J. Phys. **6**, 167 (2004).
[13] J. Geraci, Quantum Inf Process **7**, 227 (2008).
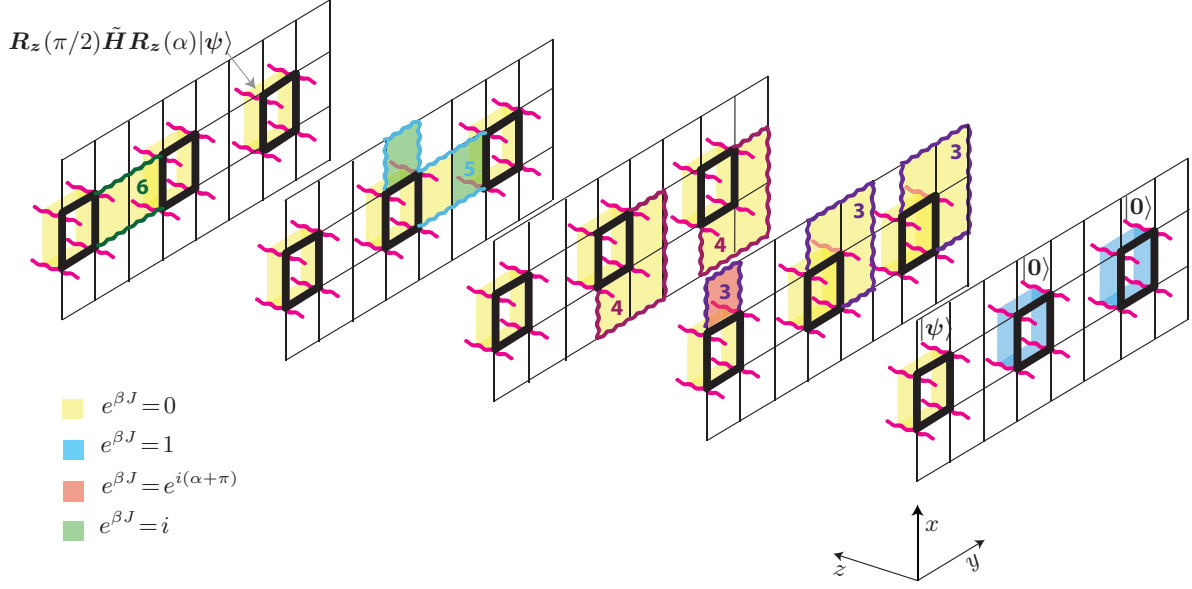[14] J. Geraci and D. A. Lidar, Commun. Math. Phys **279**, 735 (2008).

FIG. 11: Part of a circuit with $\mathbb{Z}_2$–LGT–type gates that shows the processing of a logical qubit $|\psi\rangle$. First, a logical rotation $\boldsymbol{R_z}(\alpha)$ is applied to it. Then, a logical teleportation–based Hadamard gate (up to a phase) is applied, which results in the state $\boldsymbol{R_z}(\pi/2)\tilde{\boldsymbol{H}}\boldsymbol{R_z}(\alpha)|\psi\rangle$ (see text). Note that the qubit is processed in the z direction (corresponding to time) as well as the y direction. Colored faces indicate faces where the coupling strength has a specific value, as indicated in the legend. Wavy lines indicate edges whose spins have been fixed by the gauge, and their color has no meaning nor a correlation with the color of the faces. They are a guide to the eye to verify that no loops are formed, as shown in Fig. 12.

[15] J. Geraci and D. A. Lidar, New J. Phys. **12**, 075026 (2010).
[16] S. Bravyi and R. Raussendorf, Phys. Rev. A **76**, 022304 (2007).
[17] D. Aharonov, I. Arad, E. Eban, and Z. Landau, arXiv:quant-ph/0702008 (2007).
[18] D. Aharonov and I. Arad, arXiv:quant-ph/0605181 (2006).
[19] P. Wocjan and J. Yard, Quant. Inf. Comp. **8**, 147 (2008).
[20] J. B. Kogut, Rev. Mod. Phys. **51**, 659 (1979).
[21] F. J. Wegner, J. Math. Phys. **12**, 2259 (1971).
[22] K. G. Wilson, Rev. Mod. Phys. **47**, 773 (1975).
[23] M. Van den Nest, W. Dür, R. Raussendorf, and H. J. Briegel, Phys. Rev. A **80**, 052334 (2009).
[24] A. Sokal, Surveys in combinatorics **327**, 173 (2005).
[25] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[26] J.-M. Maillard, Journal of Nonlinear Mathematical Physics **10**, 119 (2003).
[27] H. Nishimori and G. Ortiz, *Elements of Phase Transitions and Critical Phenomena* (Oxford University Press, USA, 2011).
[28] M. Creutz, Phys. Rev. D **15** (1977).
[29] D. Aharonov, V. Jones, and Z. Landau, Proc. of 38th ACM symposium on Theory of computing **427** (2006).
[30] J. Smith and M. Mosca, arXiv:1001.0767 (2010).
[31] J. E. Sacco and F. Y. Wu, J. Phys. A: Math. Gen. **8**, 1780 (1975).
[32] D. P. DiVincenzo, D. Bacon, J. Kempe, G. Burkard, and K. B. Whaley, Nature **408**, 339 (2000).
[33] M. Hsieh, J. Kempe, S. Myrgren, and K. B. Whaley, Quant. Inf. Proc. **2**, 289 (2004).
[34] Y. Shi, Quant. Inf. Comp. **3**, 84 (2003).
[35] R. Hübener, V. Nebendahl, and W. Dür, New J. Phys. **12**, 025004 (2010).
[36] G. De las Cuevas, W. Dür, H. J. Briegel, and M. A. Martin-Delgado, Phys. Rev. Lett. **102**, 230502 (2009).
[37] G. De las Cuevas, W. Dür, H. J. Briegel, and M. A. Martin-Delgado, New J. Phys. **12**, 043014 (2010).
[38] A. Gilchrist, N. K. Langford, and M. A. Nielsen, Phys. Rev. A **71**, 062310 (2005).
[39] W. Dür, M. J. Bremner, and H. J. Briegel, Phys. Rev. A **78**, 052325 (2008).
[40] A planar graph is a graph which can be drawn in the plane without crossings of the edges.
[41] This is opposite to the way quantum circuits are usually drawn, where the first processing takes place from left to right.
[42] One may also use results from fault–tolerant quantum computation, which state that also noisy gates with a small but constant error suffice to perform quantum computation. This implies that ϵ can be a small constant not depending on the size of the circuit, however additional overhead for encoding and fault-tolerant gate implementation would be required in this case.
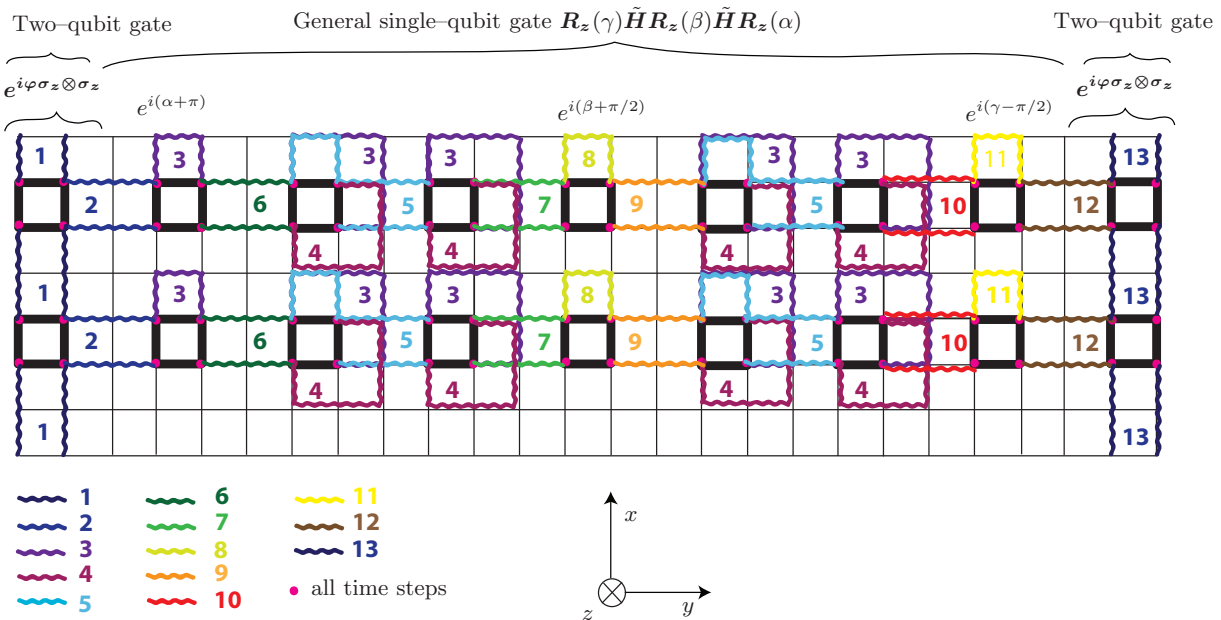
FIG. 12: A projection of the circuit of the 3D $\mathbb{Z}_2$ LGT into its spatial dimension. Part of the circuit in its normal form (that is, in the structure two–qubit gate, single–qubit gate, two–qubit gate) is illustrated. Logical qubits are indicated with thick, black lines. All edges in the time direction (going out of the paper) which are boundary to a logical qubit are fixed by the gauge (pink dots). Edges in the spatial direction are either not fixed by the gauge (black, thin lines), or are fixed by the gauge at *different* time steps $1\ldots 13$ indicated with a wavy, colored edges. Hence, a loop of edges fixed by the gauge would correspond in this figure to a closed loop of wavy, colored edges. It can be verified by inspection that no such loops are present.